

NETWORK PROTOCOLS

After reading this chapter and completing the exercises, you will be able to:

- ◆ Understand networking in Windows XP
- ◆ Understand Windows XP's networking protocols
- ◆ Configure and use TCP/IP protocols and services
- ◆ Access NetWare servers and services from Windows XP
- ◆ Understand Windows XP Remote Tools

In this chapter, we discuss the networking protocols that Windows XP supports, as well as how and when to use them. We discuss TCP/IP (Transmission Control Protocol/Internet Protocol)—probably the most important networking protocol used with any version of Windows—and what is required to configure Windows XP to employ this protocol for network communications. We also discuss NWLink, a protocol historically associated with NetWare, but a valid protocol option under Windows XP as well. We also discuss other protocols that Windows XP Professional supports.

WINDOWS XP NETWORK OVERVIEW

Windows XP is the most versatile Windows operating system from Microsoft to date. It is capable of establishing a network connection through myriad devices and technologies. Windows XP was designed specifically to offer easy-to-use networking capabilities for both inexperienced home users and enterprise-level networked organizations. Windows XP is able to act as a standalone system for occasional Internet dial-up, or as a dedicated workgroup connection-sharing server, or even as a client in a domain network.

Windows XP supports local area network (LAN) connections, which are typically established with an expansion card or a PC Card network adapter. The network medium is attached to the network adapter, usually with twisted-pair cabling. Windows XP offers both WAN and LAN support, and can establish VPN and IPSec connections with local and remote systems. Windows XP also supports a wide range of MAN and WAN communication devices.

Windows XP has improved upon the remote access support found in Windows 9x and Windows 2000. It is easier to create and use dial-up Internet connections than in previous versions. Windows XP also supports dedicated connections such as cable modems, or specialty connections such as DSL and ISDN. Through the use of the proper hardware, Windows XP can fully manage any type of remote access connectivity.

Windows XP also supports emerging wireless technologies to eliminate network cables from both home and office networking. In fact, Microsoft is so intent on pushing wireless technologies that it has transformed most of its own Redmond, Washington, campus and many of its branch offices into wireless networks. Microsoft has placed itself firmly behind the IEEE 802.11 wireless standards. Many public facilities, such as airports and hotels, are adopting wireless technologies to offer Internet connectivity and local information to their customers throughout their buildings without tying people down with wires. Once a wireless NIC is installed, you'll find that Windows XP integrates itself seamlessly into a wireless network.

Through its implementation of the NWLink protocol, Windows XP continues its support for the IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol suite for compatibility with Novell NetWare networks. There is a large installed user base for NetWare; therefore, support for this type of network transmission is important to overall network connectivity.

WINDOWS XP NETWORK COMPONENTS

Windows XP is designed for networking, with all the elements necessary for interacting with a network without requiring any additional software. Windows XP networking is powerful and efficient, while being relatively easy to configure and use with a graphical user interface and Wizards for configuration support.

Windows XP Professional can function as a network client, as a network server (in a limited sense), or both. It can participate in peer-to-peer, client/server, and terminal/host environments. Windows XP also has everything needed to access the Internet, including all necessary protocols and client capabilities, a Web browser (Internet Explorer), and other Internet tools and utilities.

In Windows XP, numerous components work together to define its networking capabilities. Each component provides one or more individual network functions and defines an interface through which data moves on its way to and from other system components. This allows Windows XP to support multiple protocols easily and transparently; applications need only know how to communicate through a standard application programming interface (API), while the modular organization of the operating system shields them from the complex details that can sometimes be involved.

Networking components can be added to or deleted from a Windows XP system without affecting the function of other components, except in those cases where such components are bound to the other components. (Binding is discussed later in this chapter.) Adding new components brings new services, communications technologies, and other capabilities into existing networks and allows additional protocols to join the mix at any time.

NETWORK PROTOCOLS

Windows XP supports two core network transport protocols. Both of these protocols can be used on any network of any size. The major network protocols are the **Transmission Control Protocol/Internet Protocol (TCP/IP)** and **NWLink** (identified in the Local Area Connection Properties window as the NWLink IPX/SPX/NetBIOS Compatible Protocol). These network protocols have associated advantages and drawbacks, as outlined in the sections that follow. The following list sums up the important characteristics of each of these protocols:

- TCP/IP works on almost any scale, from a single-segment network to a global scale, as demonstrated by its use on the global Internet. TCP/IP is complicated yet powerful, and is the most widely used of all networking protocols.
- NWLink works best on networks of medium scope (20 servers or fewer in a single facility). It's also useful on networks that include versions of NetWare that predate NetWare 5.x (the first version of NetWare to incorporate full-blown, native TCP/IP support).

TCP/IP

TCP/IP represents an all-embracing suite of protocols that cover a wide range of capabilities (more than 50 component protocols that belong to the TCP/IP suite have been standardized).

TCP/IP has also been around for a long time; the original version of TCP/IP emerged from research funded by the Advanced Research Projects Agency (ARPA, a division of the U.S. Department of Defense). Work on this technology began in 1969, continued throughout the 1970s, and became broadly available in 1981 and 1982. Today, TCP/IP is the most common networking protocol in use worldwide, and it is the protocol suite that makes the Internet possible.

TCP/IP has become the platform for a staggering variety of network services, including newsgroups (NNTP), electronic mail (SNMP and MIME), file transfer (FTP), remote printing (lpr, lpd, lpq utilities), remote boot (bootp and **DHCP—Dynamic Host Configuration Protocol**), and the World Wide Web (HTTP—Hypertext Transfer Protocol).

To provide **Network Basic Input/Output System (NetBIOS)** support using TCP/IP transports, Microsoft includes an implementation of **NBT (NetBIOS over TCP/IP)** with Windows XP. Microsoft extends the definition of NBT behaviors by defining a new type of NetBIOS network node for the NBT environment, called an “H” (for Hybrid) node. An H node inverts the normal behavior of the standard NBT “N” (or network) node. It looks first for a NetBIOS name service (such as a WINS server), then sends a broadcast to request local name resolution. An N node broadcasts first, then attempts a directed request for name resolution. Microsoft’s approach reduces the amount of broadcast traffic on most IP-based networks that use NetBIOS names (as older Microsoft networks that predate Windows 2000 must do).

TCP/IP Advantages

TCP/IP supports networking services better than the other Windows XP protocols through its multiple components (see Figure 7-1). TCP/IP supports multiple routing protocols that in turn support large, complex networks. TCP/IP also incorporates better error detection and handling, and works with more kinds of computers than any other protocol suite. The following is a list of the elements shown in Figure 7-1:

- *Other*—Any of the nearly 40 other service/application-level protocols defined for TCP/IP.
- **FTP (File Transfer Protocol)**—The service protocol and corresponding TCP/IP application that permit network file transfer.
- *Telnet*—The service protocol and corresponding TCP/IP applications that support networked terminal emulation services.
- **SMTP (Simple Mail Transfer Protocol)**—The most common e-mail service protocol in the TCP/IP environment. POP3 (Post Office Protocol version 3) and IMAP (Internet Mail Access Protocol) are also involved in a great deal of Internet e-mail traffic.
- **UDP (User Datagram Protocol)**—A secondary transport protocol on TCP/IP networks, UDP is a lightweight cousin of TCP. It is **connectionless**, has low overhead, and offers best-effort delivery rather than the delivery guarantees

offered by TCP. It is used for all kinds of services on TCP networks, including NFS and TFTP.

- **NFS (Network File System)**—A UDP-based networked file system originally developed by Sun Microsystems and widely used on many TCP/IP networks. (Windows XP does not include built-in NFS support, but numerous third-party options are available.)
- **TFTP (Trivial File Transfer Protocol)**—A lightweight, UDP-based alternative to FTP, designed primarily to permit users running Telnet sessions elsewhere on a network to grab files from their “home machines.”
- **DNS (Domain Name Service)**—An address resolution service for TCP/IP-based networks that translates between numeric IP addresses and symbolic names known formally as fully qualified domain names (FQDNs).
- **SNMP (Simple Network Management Protocol)**—The primary management protocol used on TCP/IP networks, SNMP is used to report management data to management consoles or applications and to interrogate repositories of management data around a network.
- **TCP (Transmission Control Protocol)**—The primary transport protocol in TCP/IP, TCP is a robust, reliable, guaranteed delivery, **connection-oriented** transport protocol.
- **Routing protocols**—These embrace a number of important IP protocols, including the Routing Internet Protocol (RIP), the Open Shortest Path First (OSPF) protocol, the Border Gateway Protocol (BGP), and others.
- **ARP (Address Resolution Protocol)**—Used to map from a logical IP address to a physical MAC-layer address.
- **RARP (Reverse Address Resolution Protocol)**—Used to map from a physical MAC-layer address to a logical IP address.
- **IP (Internet Protocol)**—The primary protocol in TCP/IP, IP includes network-addressing information that is manipulated when a packet is routed from sender to receiver, along with data integrity and network status information.
- **ICMP (Internet Control Message Protocol)**—The protocol that deals with quality of service, availability, and network behavior information. Also supports the **PING (Packet Internet Groper)** utility, often used to inquire if an address is reachable on the Internet, and if so, to provide a measure of the “round trip time” to send a packet to its destination address, and receive a reply.
- **IEEE 802.X**—Includes the 802.2 networking standard, plus standard networking technologies like Ethernet (802.3) and Token Ring (802.5), among others.
- **FDDI (Fiber Distributed Data Interface)**—A 100 Mbps fiber-based networking technology.

- *ATM (Asynchronous Transfer Mode)*—A cell-oriented, fiber- and copper-based networking technology that supports data rates from 25 Mbps to as high as 2.4 Gbps.
- *ISDN (Integrated Services Digital Network)*—A digital alternative to analog telephony, ISDN links support two or more 64 Kbps channels per connection, depending on type.
- *X.25*—An ITU standard for packet-switched networking, X.25 is very common outside the United States where its robust data-handling capability makes it a good match for substandard telephone networks.
- *Ethernet II*—An older version of Ethernet that preceded the 802.3 specification, Ethernet II offers the same 10 Mbps as standard Ethernet, but uses different frame formats.

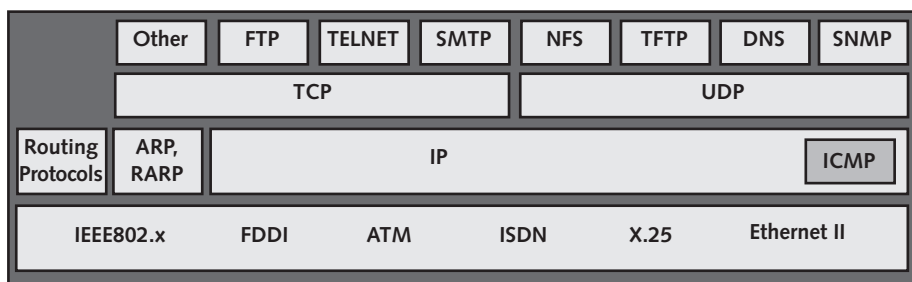


Figure 7-1 TCP/IP protocol stack

In addition to its many services and capabilities, TCP/IP also supports the following:

- Direct Internet access from any TCP/IP-equipped computer, with a link to the Internet by phone, some kind of digital link (ISDN, frame relay, T1, and so forth), or across any network with routed Internet access.
- Powerful network management protocols and services, such as SNMP and the Desktop Management Interface (DMI, which supports interrogation of desktop hardware and software configuration data).
- Dynamic Host Configuration Protocol (DHCP), which provides unique IP addresses on demand and simplifies IP address management.
- Microsoft's **Windows Internet Name Service (WINS)** to enable IP-based NetBIOS name browsing for Microsoft clients and servers, as well as the Domain Name Service (DNS) that is the most common name resolution service used to map FQDNs to numeric IP addresses throughout the Internet. NetBIOS names are limited to 15 characters. FQDNs or HOST names are names comprised of multiple segments, such as mail.adminsys.microsoft.com.

The Internet Network Information Center (InterNIC) manages all TCP/IP domain names, network numbers, and IP addresses, to make the global Internet work correctly and reliably.

TCP/IP Drawbacks

For all the clear advantages of TCP/IP, there are some drawbacks. As network protocols go, TCP/IP is neither extremely fast nor terribly easy to use. Configuring and managing a TCP/IP-based network requires a fair degree of expertise, careful planning, and constant maintenance and attention. Each of the many services and protocols that TCP/IP supports brings its own unique installation, configuration, and management chores. In addition, there's a huge mass of information and detail work involved in establishing and maintaining a TCP/IP-based network. In short, it's a demanding and unforgiving environment, and should always be approached with great care.

7

NWLink (IPX/SPX)

NWLink is Microsoft's implementation of Novell's **IPX/SPX** protocol stack. Rather than supporting the native Novell **Open Datalink Interface (ODI)**, NWLink works with the **NDIS (Network Device Interface Specification)** driver technology that's native to Windows XP; NDIS defines parameters for loading more than one protocol on a network adapter. NWLink is sufficiently complete to support the most important IPX/SPX APIs.



Although IPX/SPX is the default protocol for NetWare prior to version 5, TCP/IP is the default protocol in version 5.

NWLink Advantages

NWLink offers some powerful capabilities, including:

- *SPX II*—SPX II is a new version of SPX that has been enhanced to support windowing and can set a maximum frame size.
- *Auto detection of frame types*—NWLink automatically detects which **IPX frame type** is used on a network during initial startup and broadcast advertisement phases. When multiple frame types appear, Windows XP defaults to the industry-standard 802.2 frame type.
- *Direct hosting over IPX*—This is the ability to host ongoing network sessions using IPX transports. Direct hosting over IPX can increase network performance by as much as 20 percent on client computers. This is especially beneficial for client/server applications.

NWLink Drawbacks

On large networks, IPX may not scale well. IPX lacks a built-in facility for centralized name and address management like the service that DNS provides for TCP/IP. This omission allows address conflicts to occur—especially when previously isolated networks that employed identical defaults or common addressing schemes attempt to interoperate. Novell established an address Registry in 1994 (IPX was introduced in 1983), but it is generally neither used nor acknowledged. The InterNIC and its subsequent assigns have managed all public IP addresses since 1982. IPX fails to support a comprehensive collection of network management tools. Finally, IPX imposes a greater memory footprint on DOS machines and runs less efficiently across slow serial connections.

NetBEUI and DLC

Both **NetBIOS Extended User Interface (NetBEUI)** and **Data Link Control (DLC)** have been greatly de-emphasized in Windows XP. In fact, you won't even find them as available options when attempting to install new protocols. Microsoft has finally seen the light. NetBEUI is not often used anymore, owing to its limitations on the number of addressable nodes per network and its inability to be routed. Likewise, DLC has been replaced by SNA for mainframe interaction and TCP/IP or proprietary protocols for network attached printers. If your current network relies upon either of these protocols, you need to consider other alternatives before deploying Windows XP.

INTERPROCESS COMMUNICATION

In the Windows XP environment, communication among processes is quite important because of the operating system's multitasking, multithreaded architecture. **Interprocess communication (IPC)** defines a way for such processes to exchange information. This mechanism is general-purpose so it doesn't matter whether such communications occur on the same computer or between networked computers. IPC defines a way for client computers to request services from some servers and permits servers to reply to requests for services. As shown in Figure 7-2, IPC operates directly below the redirector on the client side and the network file system on the server side to provide a standard communications interface for handling requests and replies.

In Windows XP, IPC mechanisms fall into two categories: programming interfaces and file system mechanisms. Programming interfaces permit general, open-ended client/server dialog, as mediated by applications or system services. Normally, such dialog is not strictly related to data streams or data files. File system mechanisms support file sharing between clients and servers. Where programming interfaces are concerned, individual APIs differ depending on what kinds of client-server dialog they support. Where file systems are concerned, they must behave the same way, no matter how (or where) they employ Windows XP networked file systems and services.

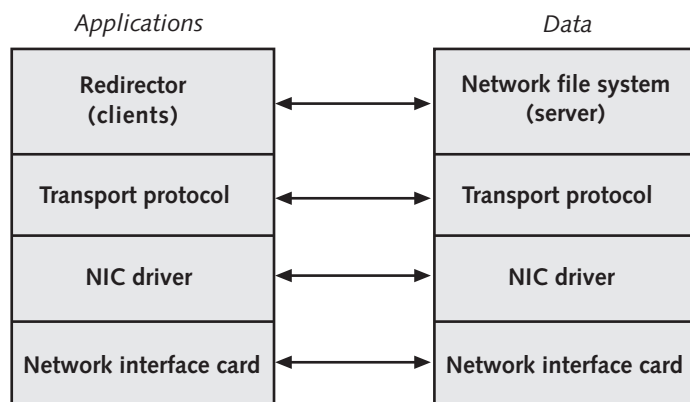


Figure 7-2 Interprocess communication between client and server

IPC File System Mechanisms

Windows XP includes two IPC interfaces for file system access: named pipes and mail-slots. These mechanisms work through the Windows XP redirector, which distinguishes between local and network resource requests. This process permits one simple set of file I/O commands to handle both local and network access to file system data.

Named Pipes

Named pipes support a connection-oriented message-passing service for clients and servers. To be connection-oriented, a message's receiver must acknowledge each message it receives. Named pipes offer a reliable method for clients and servers to exchange requests, replies, and associated files. Named pipes provide their own methods to ensure reliable data transfer, which makes them a good match for lightweight, unreliable transport protocols like the User Datagram Protocol (UDP). In short, named pipes delivery guarantees make transport-level delivery guarantees less essential.

The Windows XP version of named pipes includes a security feature called impersonation, which permits the server side of the named pipes interface to masquerade as a client that requests a service. This allows the interface to check the client's access rights and to make sure that the client's request is legal, before returning any reply to request for data.

Mailslots File System

Mailslots are like a connectionless version of named pipes; mailslots offer no delivery guarantees, nor do they acknowledge successful receipt of data. Windows XP uses mailslots internally to support nonessential system-to-system communications. Such things as registering names for computers, domains, and users across a network, passing messages related to the Windows XP browser service, and providing support for broadcasting text

messages across the network fall into this category. Outside such lightweight uses, mail-slots are used less frequently than named pipes.

IPC Programming Interfaces

For communications to succeed, the client and server sides of an application must share a common programming interface. Windows XP offers a number of distinct interfaces to support IPC mechanisms for various kinds of client/server applications. Windows XP supports several programming interfaces, including NetBIOS, Windows Sockets, RPC, NetDDE, DCOM, Wnet, and WinInet.



External applications can support other programming interfaces or implement private interfaces.

NetBIOS

NetBIOS is a widely used, but simple PC client/server IPC mechanism. Because it is so easy to program, it has remained quite popular ever since IBM published its definition in 1985. NetBIOS services are required to permit older Windows networks to operate, or to permit older clients and servers (those that predate Windows 2000 and Windows XP) to operate on a Microsoft Windows network.

Fortunately, NetBIOS works with all TDI-compliant transports, including NWLink (NetBIOS over NWLink, or NWNBLink) and TCP/IP (NetBIOS over TCP/IP, or NBT). Windows XP uses TCP/IP as its primary network protocol by default, but Windows XP may also use NBT. By default, Windows XP's TCP/IP is configured to use the NetBIOS setting defined by a local DHCP server. However, when statically defined IP addresses are used, NetBIOS is enabled by default. This setting is configured on the WINS tab of the Advanced TCP/IP Properties dialog box. The options here are:

- Use NetBIOS setting from the DHCP server. If a static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP (selected by default)
- Enable NetBIOS over TCP/IP
- Disable NetBIOS over TCP/IP

Windows Sockets

Windows Sockets (WinSock) define a standardized and broadly deployed interface to network transports such as TCP/IP and IPX. WinSock was created to migrate UNIX applications written to the Berkeley Sockets specification into the Windows environment. WinSock also makes it easier to standardize network communications used on multiple platforms because one socket interface is much like another, even if one runs on UNIX and the other on some variety of Windows (such as Windows XP, where WinSock 2.0 is the standard sockets API).

Windows Sockets appear in many programs that originated as UNIX programs and include the majority of Internet utilities, especially the most popular IP utilities, such as Web browsers, e-mail software, and file transfer programs.

RPC

Remote Procedure Call (RPC) implements IPC tools that can invoke separate programs on remote computers, supply them with input, and collect whatever results they produce. This permits the distribution of a single processing task among multiple computers, a process that can improve overall performance and help balance the processing load across numerous machines.

RPC is indifferent to where its client and server portions reside. It's possible for both client and server portions of an application to run on a single computer. In that case, they communicate using local procedure call (LPC) mechanisms. This makes building such applications easy because they can be constructed on one computer, while allowing processing to be distributed on one machine or across many machines, as processing needs dictate. This creates an environment that is both flexible and powerful.

RPC consists of four basic components:

- A remote stub procedure that packages RPC requests for transmission to a server. It's called a stub because it acts as a simple, extremely compact front end to a remote process that may be much larger and more complex elsewhere on the network.
- An RPC runtime system to pass data between local and remote machines or between client and server processes.
- An application stub procedure that receives requests from the runtime RPC system. Upon such receipt, this stub procedure formats requests for the designated target RPC computer and makes the necessary procedure call. This procedure call can be either a local procedure call (if both client and server components are running on the same computer) or a remote procedure call (if client and server components are running on two machines).
- One or more remote procedures that may be called for service (whether locally or across the network).

NetDDE

Network Dynamic Data Exchange (NetDDE) creates ongoing data streams called exchange pipes (or simply, pipes) between two applications across a network. This process works just like Microsoft's local **DDE**, which creates data exchange pipes between two applications on the same machine. DDE facilitates data sharing, object linking and embedding (OLE), and dynamic updates between linked applications. NetDDE extends local DDE across the network.

NetDDE services are installed by default during the base Windows XP installation, but they remain dormant until they are started explicitly. NetDDE services must be started using the Services control in Computer Management, where they appear under the headings Network DDE (the client side of NetDDE) and Network DDE DSDM (DDE Share Database Manager, the server side of NetDDE).

Distributed Component Object Model

Distributed Component Object Model (DCOM) (previously known as Network OLE) is a protocol that facilitates the communication of application components over a network by providing a reliable, secure, and efficient mechanism for exchanging information. DCOM can operate over most network transport mechanisms, including HTTP. Microsoft based its implementation of DCOM on the Open Software Foundation's DCE-RPC specification, but expanded its capabilities to include Java and ActiveX support.

Windows Network Interface

The Windows Network (Wnet) interface allows applications to take advantage of Windows XP networking capabilities through a standardized API. This means that the application does not require specific control data about the network provider or implementation, allowing applications to be network-independent while still able to interact with network-based resources.

Win32 Internet API

The WinInet API (WinInet) is a mechanism that enables applications to take advantage of Internet functionality without requiring extensive proprietary programming. Through WinInet, applications can be designed to include FTP, Web, and Gopher support with a minimal of additional coding. WinInet makes interacting with Internet resources as simple as reading files from a local hard drive without requiring programming to WinSock or TCP/IP.

REDIRECTORS

A redirector examines all requests for system resources and decides whether such requests are local (they can be found on the requesting machine) or remote. The redirector handles transmission of remote requests across the network so that the requests are filled.

Windows XP's file and print sharing are regarded as the most important functions supplied by any network operating system. Windows XP delivers these services through two critical components: the Workstation service and the Server service. Both of these services are essentially file system drivers that operate in concert with other file system drivers that can access local file systems on a Windows XP machine. The following components are redirectors that operate at this level: Workstation service, Server service, **Multiple Universal Naming Convention Provider (MUP)**, and **Multi-Provider Router (MPR)**.

All of these system components take client requests for service and redirect them to an appropriate network service provider. Redirectors interact and interface directly with user applications. The sections that follow explain more about each of these components and their roles in the Windows XP networking environment.

Workstation Service

The Workstation service supports client access to network resources and handles functions such as logging in, connecting to network shares (directories and printers), and creating links using Windows XP's IPC options. The Workstation service has two elements, the User mode interface and the redirector. The User mode interface determines the particular file system that any User mode file I/O request is referencing. The redirector recognizes and translates requests for remote file and print services and forwards them to lower-level boundary layers aimed at network access and delivery.

This service encompasses a redirector file system that handles access to shared directories on networked computers. The file system is used further to satisfy remote access requests, but if any request uses a network name to refer to a local resource, it will instead pass that request to local file system drivers.

The Workstation service requires that at least one TDI-compliant transport and at least one MUP are running. Otherwise, the service cannot function properly because it supports connections with other Windows XP machines (through their Server services), LAN Manager, LAN Server, and other MS-Net servers, which require an MUP to be running. The Workstation service, like any other redirector, communicates with transport protocols through the common TDI boundary layer.

Server Service

The Windows XP Server service handles the creation and management of shared resources and performs security checks against requests for such resources, including directories and printers. The Server service allows a Windows XP computer to act as a server on a client/server network, up to the maximum number of licensed clients. This limits the number of simultaneous connections possible to a Windows XP Professional machine to 10, in keeping with its built-in connection limitations.

Just as with the Workstation service, the Server service operates as a file system driver. Therefore, it also uses other file system drivers to satisfy I/O requests. The Server service is also divided into two elements:

- *SERVER.EXE*—Manages client connection requests.
- *SRV.SYS*—The redirector file system that operates across the network, and that interacts with other local file system drivers when necessary.

Multiple Universal Naming Convention Provider

Windows XP supports multiple redirectors that can be active simultaneously. As an example, both the Workstation and Server services and the NetWare redirector built into Windows XP's **Client Service for NetWare (CSNW)** can be active at the same time. Like the Server service, the NetWare redirector handles Microsoft Windows Network shares, but exposes them to NetWare clients instead of Microsoft Network clients. As with other boundary layers, the ability to support multiple clients uniformly is possible because a common provider interface allows Windows XP to treat all redirectors the same way.

The boundary layer called the Multiple Universal Naming Convention Provider (MUP) defines a link between applications that make UNC requests for different redirectors. MUP allows applications to remain oblivious to the number or type of redirectors that might be in use. For incoming requests, the MUP also decides which redirector should handle that request by parsing the UNC share name that appears within the request.

Here's how it works: When the I/O subsystem receives any request that includes a UNC name, it turns that request over to the MUP. The MUP first checks its internal list of recently accessed shares, which it maintains over time. If the MUP recognizes the UNC name, it immediately passes the request to the required redirector. If it doesn't recognize the UNC name, the MUP sends the request to each registered redirector and requests that it service the request.

The MUP chooses redirectors on the basis of the highest registered response time during which the redirector claims it can connect to a UNC name, information that can be cached until no activity occurs for 15 minutes. This can make trying a series of redirectors incredibly time-consuming and helps explain why the binding order of protocols is so important, because that also influences the order in which name resolution requests will be handled.

Universal Naming Convention Names

Universal Naming Convention (UNC) names represent the format used in NetBIOS-oriented name resolution systems. UNC names precede the computer portion of a name with two slashes, followed by a slash that precedes (and separates elements of) the share name and the directory path, followed by the requested file name. Thus this string

```
\\computername\sharename\dir-path\filename.ext
```

represents a valid UNC name. In this example, the name of the computer is *computer-name*, the name of the share is *sharename*, the directory path is named *dir-path*, and the file is named *filename.ext*.

Multi-Provider Router

Not all programs use UNC names in the Windows XP environment. Programs that call the Win32 API must use the file system service called the **Multi-Provider Router**

(MPR) to designate the proper redirector to handle a resource request. The MPR lets applications written to older Microsoft specifications behave as if they were written to conform to UNC naming. The MPR is able to recognize the UNC's that represent drive mappings, so it can decide which redirector can handle a mapped network drive letter (such as X:) and make sure that a request that references that drive can be properly satisfied. The MPR handles all Win32 Network API calls, passing resource requests from that interface to those redirectors that register their presence through special-purpose dynamic link libraries (DLLs). That is, any redirector that wants to support the MPR must provide a DLL that communicates through the common MPR interface. Normally this means that whichever network developer supplies a redirector must also supply this DLL. Microsoft implemented CSNW as a DLL that supports this interface. This allows the NetWare redirector to provide the same kind of transparent file system and network resource access as other Windows XP redirectors.

NETWORKING UNDER WINDOWS XP

The Windows XP networking system is controlled by a single multifaceted interface that combines networking access for LAN, Internet, and modem. The interface is called Network Connections (see Figure 7-3), and is accessed through the Control Panel (in Classic View, or through the Network and Internet Connections category in Category View). A Connect To submenu is added to the Start menu if you create dial-up or VPN connection objects. Through this menu, you can also access the Network Connections tool by selecting the Show all connections command.

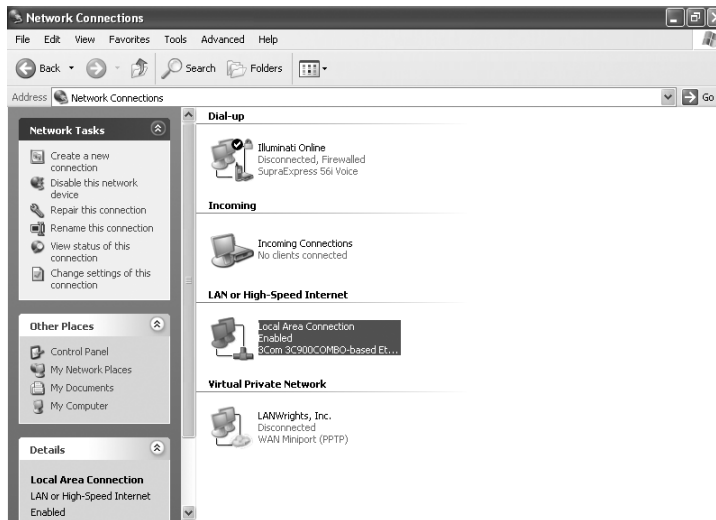


Figure 7-3 The Network Connections utility

Network Connections is used to create and configure network connections. The “Create a new connection” command in the Network Tasks list launches a Wizard that takes the user through the process of establishing new network links. The Wizard is used for any network links employing modems, virtual private networks (VPNs) over the Internet, or serial, parallel, or infrared ports. Windows XP automatically enables all normal network links achieved through a network adapter and an attached cable. A Local Area Connection icon is listed in the Network Connections window for each installed adapter card. If there are two or more LAN connections, we recommend renaming the Local Area Connection icons to reflect the domain, network, or purpose of the link.

Existing Local Area Connections can be configured by opening the Properties for that object either through the File menu or the right-click pop-up menu. A typical default configuration of a Local Area Connection Properties dialog box is shown in Figure 7-4, listing the adapter in use as well as all installed protocols and services that can function over this interface. The Configure button is used to access the Properties dialog box for the adapter. Each listed service or protocol has a checkbox. When checked, the protocol or service is bound to the adapter (that is, it can operate over the network link established by the adapter). When unchecked, the protocol or service is not bound to the adapter.

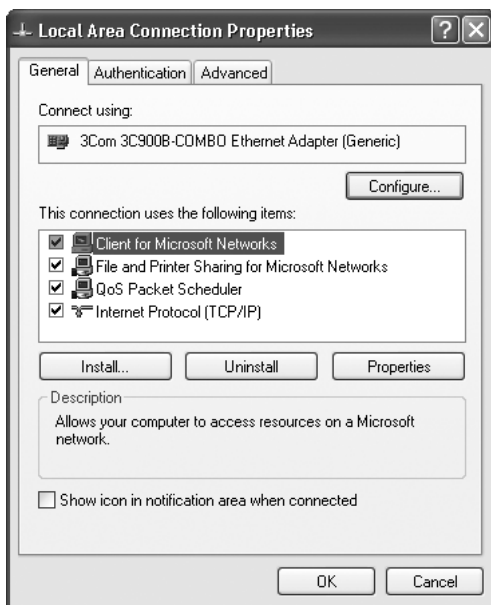


Figure 7-4 A Local Area Connection Properties dialog box, General tab

The Install button is used to add new client interfaces, protocols, and services that any of the Connection objects can use. When a new element is added, all possible bindings

are enabled by default. The following are the available elements that can be installed onto Windows XP Professional:

- *Client: Client for Microsoft Networks*—Used to gain access to Microsoft network resources. This component is installed by default.
- *Client: Client Service for NetWare*—Used to gain access to NetWare resources.
- *Service: QoS Packet Scheduler*—An extension service for Winsock used to reserve bandwidth for communications. This component is installed by default.
- *Service: File and Printer Sharing for Microsoft Networks*—Enables a system to share its files and printers with a Microsoft network. This component is installed by default.
- *Service: Service Advertising Protocol*—Used by Windows XP to participate actively in NetWare networks.
- *Protocol: Internet Protocol (TCP/IP)*—Protocol used on networks connected to the Internet or using Internet Information Services (IIS) privately. This component is installed by default.
- *Protocol: Network Monitor Driver*—Driver used to allow full versions of Network Monitor to obtain network activity information from Windows XP Professional systems.
- *Protocol: NWLink IPX/SPX/NetBIOS Compatible Transport Protocol*—Protocol most often used on NetWare networks.

The Uninstall button is used to remove a client, protocol, or service. Once an element is removed, it is removed for all Connection objects. The Properties button opens the Properties dialog box for the selected installed component (client, service, or protocol). Note that not all components have configurable options. This dialog box also offers a checkbox control to display an icon in the icon tray when the Connection object is in use.

The Network Connections interface's File and Advanced drop-down menus include the following functions:

- *File: Disable*—Prevents the selected Connection object from being used to establish a communications link. This command is for automatic connections, such as those for a LAN.
- *File: Enable*—Allows the selected Connection object to be used to establish a communications link. This command is for automatic connections, such as those for a LAN.
- *File: Connect*—Launches the selected Connection object to establish a communications link. This command is for manual connections, such as those over a modem.

- *File: Status*—Displays a Status window for the selected Connection object that lists whether the object is connected, how long the connection has been active, the speed of the connection, and the packet counts. This window offers Properties and Disable buttons to perform the same functions as the File menu commands.
- *File: Repair*—Attempts to repair a connection object by clearing the ARP cache and resetting buffers or ports. This is often a good first step to try before changing configuration data. This command also forces a new DHCP lease request if the interface is configured to use DHCP.
- *File: New Connection*—Launches the Make New Connection Wizard.
- *Advanced: Operator-Assisted Dialing*—Used to manually dial a connection number then have the computer take over control of the line once the remote system answers the call.
- *Advanced: Dial-up Preferences*—Opens a dialog box in which RAS-related controls are set (see Chapter 8, “Internetworking with Remote Access”).
- *Advanced: Network Identification*—Opens the Computer Name tab of the System applet that displays the current computer name and workgroup/domain name. To join a domain and create a local user, click Network ID.
- *Advanced: Bridge Connections*—Used to create a virtual bridge between two or more network segments.
- *Advanced: Advanced Settings*—Opens a dialog box where bindings and provider order can be managed; see the “Managing Bindings” section later this chapter.
- *Advanced: Optional Networking Components*—Adds other networking components, such as Monitoring and Management Tools, Networking Services, and Other Network File and Print Services.

Some of these commands appear only when a specific Connection object type is selected.



For most networks, the default Local Area Connection Windows XP creates automatically is sufficient for LAN activity. As shown earlier in Figure 7-4, this Connection object is designed to link up with a Microsoft-based network (workgroup or domain), allows file and printer sharing, and employs the TCP/IP protocol.

To change TCP/IP settings, select the protocol from the list of components in the Properties window of a Local Area Connection, then click Properties. This reveals the Internet Protocol (TCP/IP) Properties dialog box (see Figure 7-5). From here you can easily enable DHCP for this computer, or define a static IP address, subnet mask, and gateway. You can also define the preferred and alternate DNS servers. The Advanced button brings up a multi-tabbed dialog box in which multiple IP addresses, additional gateways, DNS and WINS functionality, and TCP/IP service extension properties can be defined.

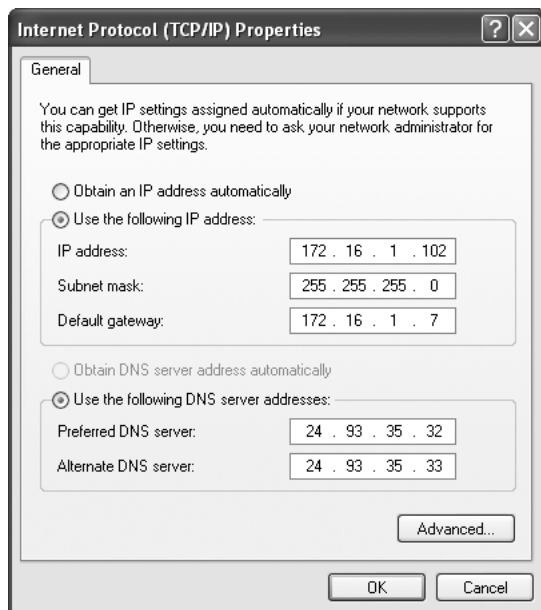


Figure 7-5 The Internet Protocol (TCP/IP) Properties dialog box

Adding new network interfaces to Windows XP Professional is handled in the same fashion as installing any other piece of hardware: physically install it and allow Windows XP to detect it and install drivers, or use the Add Hardware applet to perform the drive installation manually. Both of these procedures are discussed in Chapter 3, “Using the System Utilities.” Once a new NIC is installed, Windows XP automatically creates a new Local Area Connection that you can customize for your networking needs.

NETWORK BRIDGE

Windows XP boasts a new networking feature known as network bridge. In essence, network bridge creates a layer 2 bridge between two or more network interfaces, effectively connecting multiple network segments. Network bridge is able to connect network segments even if they use different protocols and different topologies. Microsoft has included the network bridging capability in Windows XP to help encourage the creation of networks both in small offices and at home. Using the Windows XP-based network bridge, there’s no need to purchase a separate (and sometimes expensive) hardware bridge or router. Furthermore, no configuration is required. Just select two or more network connections, then issue the Bridge Connections command from the Advanced menu in the Network Connections utility.

Windows XP can support only a single network bridge per system. However, that one bridge can bridge multiple networks together. The only restrictions on connections that

may be bridged apply to those that the Internet Connection Sharing (ICS) or Internet Connection Firewall (ICF) control. Another restriction is that only similar interfaces can be bridged. That is, a dial-up connection can be bridged only to other dial-up connections.



See Chapter 8, “Internetworking with Remote Access,” for details on ICS and ICF.

Once a bridge is created, it appears as a connection object named Network Bridge within the Network Connections utility. To add other connections to this bridge, mark their respective checkboxes in the list of adapters available in the Properties dialog box of the Network Bridge. To remove a connection from a bridge, de-select the appropriate checkbox from this dialog box. To remove the bridge altogether, select it within the Network Connections and press the Delete key.

NETWORKING WIZARD

The Network Setup Wizard (previously known as the Home Networking Wizard) is used to configure non-domain networks for small offices or home use of Windows XP. This step-by-step walk-through tool allows easy configuration of:

- Friendly computer names, such as “Study Computer” or “Den System”
- Your Internet connection, be it dial-up or dedicated
- Internet Connection Sharing (ICS)
- Internet Connection Firewall (ICF)
- Configure TCP/IP for networking

The Network Setup Wizard can be launched from the network tasks list from within the Network Connection utility, or through the Network and Internet Connections category of the Control Panel. For best results, use the Wizard on the system to be the ICS host first. All other systems on the network automatically configure themselves against the ICS host to gain access to the shared Internet link and to share resources between networked systems.

During the Network Setup Wizard’s operation, you are asked whether to create a floppy disk to run the Network Setup Wizard on Windows 98, 98 SE, or Me. If you are using any of these systems on your network, creating the floppy disk is a good idea. The Wizard will not function on any other system, thus, Windows 2000 and NT systems must be configured manually to participate in this type of network.

MANAGING BINDINGS

Binding refers to the order in which Windows XP networking components are linked. These linkages and the order in which multiple components link to a single boundary layer affect how the systems behave and how well they perform. Binding is defined in the Advanced Settings dialog box (see Figure 7-6). This dialog box is reached by issuing the Advanced Settings command from the Advanced menu of the Network Connections window.

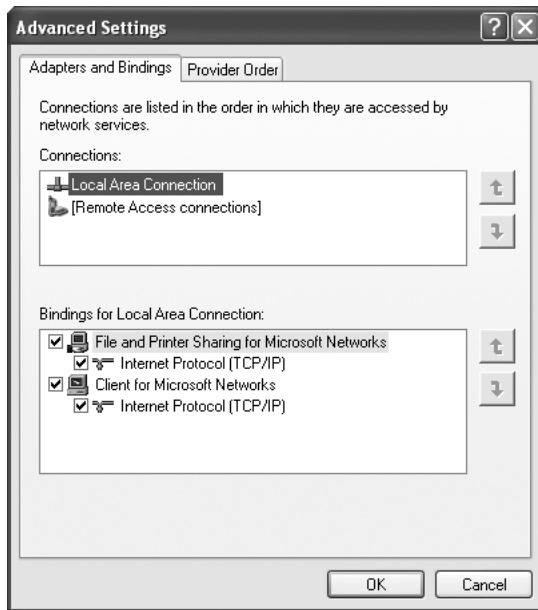


Figure 7-6 The Advanced Settings dialog box, Adapters and Bindings tab

By default, Windows XP binds any two components that share a common boundary layer, unless such bindings are explicitly removed. In fact, Windows XP binds all components that share a common boundary to the boundary layer they share, unless one or more of these bindings is removed manually.

Because this default is known as *complete binding*—that is, all possible bindings are created automatically—it can lead to system inefficiencies, especially when bindings are created that will not be used. Such unused bindings might appear higher in the binding order (as indicated by their position beneath a boundary layer element, where closer indicates higher priority) than bindings that are used. This arrangement can build delays into the system because the MUP attempts to satisfy UNC requests for names it does not recognize in the order in which bindings appear, and unused bindings must time out before the next binding in the order is attempted.

Disabling all protocol bindings that are not needed or used improves system performance and decreases the likelihood of communication errors. It's also important to understand that because clients (in this case Windows XP Professional machines) initiate communications with Windows Servers, changing the binding order of protocols on clients is what matters. Servers respond using whatever protocol appears within the transmission, so changing their binding order doesn't do much to improve performance. Changing a client's binding order, on the other hand, can sometimes deliver dramatic performance improvements.

Binding priority affects network performance because Windows XP makes connections in the order in which protocols are bound. For two machines that use IPX/SPX and TCP/IP, Windows XP uses whichever protocol appears higher in the services binding list. If both computers run IPX/SPX and TCP/IP, and IPX/SPX ranks higher than TCP/IP in the binding list, they will establish a faster connection (IPX/SPX is faster than TCP/IP) than if the bindings were reversed. To change the priority for any transport protocol, highlight an object on the Adapters and Bindings tab, then use the arrow buttons to increase (or decrease) its priority level. You can also unbind services and protocols by unselecting the checkbox in front of the object's name.

The Provider Order tab is used to alter the binding priority of various providers, such as network connectivity or print servers. This is useful only when two or more providers of the same type can be employed by a system. For example, if a computer participates in NetWare and Microsoft networking environments, it can be useful to change the priority of those providers to favor the most often accessed network.

TCP/IP ARCHITECTURE

TCP/IP supports easy cross-platform communications and provides the technical foundation for the worldwide Internet. TCP/IP is actually a suite of protocols; in this discussion, we break it down into IP and TCP. Under each of these protocols lie many additional protocols that give the TCP/IP suite such a wide range of functionality.

Internet Protocol

The Internet Protocol (IP) provides source and destination addressing and routing in the TCP/IP suite. IP addresses are logical addresses that are 32 bits (4 bytes) long. Each byte, or octet, is represented by a decimal number from 0 to 255 and separated by a period, for example, 183.24.206.18. IP is a connectionless datagram protocol that, like all connectionless protocols, is fast but unreliable. IP assumes that other protocols will be available to ensure reliable delivery of the data.



In the final octet of an IP address, the numbers 0 and 255 are reserved for special purposes. In the range of 0-255, the zero address is reserved to identify the network and the 255 address is used for broadcasts that are read by all IP hosts on the network. IP network hosts can use only numbers 1 through 254 in the final octave. “Host” is the IP-specific term that identifies any device on an IP network that is assigned a specific address.

Part of the IP address assigned to a computer designates which network the computer is on; the remainder of the address represents the host ID of that computer. The four bytes that IP uses for addresses can be broken up in multiple ways; in fact, several classes of IP addresses have been defined that use different boundaries for the network part and the host ID part. These are shown in Table 7-1.

Table 7-1 Classes of IP Addresses

Class	Network IDs	Host IDs	Usable Network IDs
A	126	16,777,214	1-126
B	16,328	65,534	128.1-191.255
C	2,097,150	254	192.0.1-223.255.254

In a Class A address, the first octet is used to identify the network and the three trailing octets are used to identify the hosts. This creates a situation in which a small number of networks (126, to be exact) is possible, but a large number of hosts (over 16 million per network) can be defined on each. Class B addresses split the octets evenly, so the first two identify the network and the second two identify the host. This permits over 16,000 networks with over 65,000 hosts. Class C addresses use the first three octets for the network portion and the final octet for the host portion of an address. This permits over two million networks, but only a maximum of 254 hosts for each Class C network.

For example, if a computer has an address of 183.24.206.18, that indicates it is a Class B address because the first two octets fall in the range of 128.1-191.255, as indicated in the fourth column of Table 7-1. Thus, the first two octets represent the network address (183.24) and the host address portion is 206.18. The computer next to it might have the address of 183.24.208.192, which indicates that it's on the same network (183.24) but has a different host address (208.192).

IP uses a special bit mask called a subnet mask to determine which part of an address denotes the network and which part the host. The job of the **subnet mask** is to block out the network section of the address so that only the host ID portion remains significant. For the addresses on the 183.24 network, the subnet mask can be stated as 255.255.0.0. Notice that the two most significant octets are occupied by a binary value that translates into all ones (255 is 11111111 in binary), while the network portion is all zeros (0 is the same as 00000000 in binary).

A subnet can be written in at least two different ways. Until recently, the most common method was to write out the subnet in dotted-decimal notation, such as 255.255.0.0. This method is the form required when configuring most systems to use TCP/IP. However, a new method for writing the subnet is simply added on to an IP address, such as 172.16.1.1/16. The slash and the number at the end of this IP address indicate the subnet mask used. The number defines the number of bits taken from the 32-bit binary form of the IP address to be used as the subnet mask. So, a /16 would be a subnet mask of 255.255.0.0 and a /24 would be 255.0.0.0.



Sometimes IP network administrators use part of what the IP address class considers the host portion of an address to further subdivide a single Class A, B, or C network. You might see the occasional subnet mask that looks like 255.192 for a Class A network, 255.255.192 for a Class B network, and 255.255.255.192 for a Class C network. 191 equals 11000000 in binary, so this extends the network portion two digits into the host ID portion of the address and permits defining two **subnets** within a single range of host addresses. The top and bottom values (0 and 3, in this case) are reserved to identify the subnetwork and to handle broadcasts, respectively.

Another form of addressing is increasingly used on the IP network, especially when individual networks don't need, or can't use, an entire Class B or Class C address. This technique is called Classless Interdomain Routing (CIDR), pronounced "cider." CIDR uses the same technique described in the preceding paragraph to let Internet service providers carve up their available addresses into more numerous subnetworks and make better use of the IP address space that's still available.

All TCP/IP addresses must be unique on the Internet—and in fact, on any IP-based network. If two IP addresses are duplicated, neither machine with that address will be able to access the network. That's why managing IP addresses is very important. At present, this responsibility falls under the aegis of the Internet Network Information Center (InterNIC). All the Class A addresses were handed out years ago, most Class Bs have been allocated, and Class C addresses are becoming scarce. (When you add together all possible networks allowed by all three address classes, you get the maximum number of individual networks on the Internet—2,113,604.) Given the vast number of networks on the Internet and the continuing growth in that arena, it is clear that subnet masking tricks and CIDR represent stopgap measures to extend the current address space as much as possible. At the same time, the standards body that governs the Internet (the IAB, or Internet Activities Board) is working to complete a new version of TCP/IP called IPv6 (the current version is IPv4), which extends the IP address space significantly. (The address space expands to 128 bits with IPv6, compared to the current 32 bits; this is enough to support trillions of networks with trillions of nodes per network.)



All IP-based devices on a single network segment must use the same subnet mask.

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is used to send control messages (such as error messages, quality of service information, and confirmations) between IP hosts. PING is used to request a response from a remote host. It uses ICMP to return messages regarding this function, such as whether the response was received or timed out, or the host was not reachable.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical (IP) address to a physical (MAC) address. When a system begins a conversation with a host for which it does not have a physical address, the system sends an ARP broadcast packet requesting a physical address that corresponds to the logical address. Given this information, the packet can be correctly sent across a physical network.



Ethernet is the common form of network in use, and on most networks the MAC address is identical to the Ethernet address. The Ethernet address takes a form represented as 00:00:00:00:00:00, or six hexadecimal digits separated by colons. In other words, on an Ethernet network, the physical (or MAC) address is the same as the Ethernet address burned into PROM on the network interface card that attaches a computer to a network. On other types of networks, the interfaces also supply unique MAC layer addresses, but their formats vary according to the kind of network in use.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is used to automatically configure computers. A DHCP server manages a defined block of IP addresses that can be assigned to computers upon request. Client systems basically take out a lease on an address, and can use that address only so long as the lease remains valid. The DHCP server handles granting, renewing, or canceling such leases. It can also block out reserved IP addresses within a numeric range, permitting certain computers that may not be able to communicate with the DHCP server to obtain static, fixed IP address assignments.

Using DHCP makes it easy for network administrators to manage IP addresses, and makes it automatic for users to gain access to IP-based resources. DHCP has proven to be a real boon for those reasons, and one of the best features of Windows XP is that it can be configured for TCP/IP by selecting the Obtain an IP address automatically radio button on the IP Protocol Properties dialog box.

Transmission Control Protocol

Transmission Control Protocol (TCP) is the primary Internet transport protocol. It accepts messages of any length and provides transportation to a TCP peer on a remote network host. TCP is connection-oriented, so it provides more reliable delivery than connectionless IP. When a connection is established, a TCP port number is used to determine

which process on the designated host is to receive any particular packet. TCP is responsible for message fragmentation and reassembly. It uses a sequencing function to ensure that packets are reassembled in the correct order and includes mechanisms both to acknowledge successful delivery of correct packets, and to request retransmission of damaged or lost packets.

UDP

User Datagram Protocol (UDP) is a connectionless protocol. Due to its reduced overhead, it is generally faster, although less reliable, than TCP. UDP was designed primarily to transport purely local services, where it is relatively safe to assume network reliability. This is one reason why it's used for distributed file systems like the Network File System (NFS) and for the Trivial File Transfer Protocol (TFTP), where the underlying assumption is that access is either purely local (NFS) or that guaranteed delivery is not required (TFTP).

FTP

File Transfer Protocol (FTP) provides file transfer services, as well as directory and file manipulation services, such as list directory contents, delete file, and specify file format.



A command-line version of FTP is available as part of Windows XP. To learn more about this command, open a DOS window (Start|All Programs|Accessories|Command Prompt) and enter `FTP ?` at the command line. This produces the Help file for that command.

Telnet

Telnet is a remote terminal emulation protocol that is primarily used to provide connectivity between dissimilar systems (PC and VAX/VMS, PC and router, UNIX and VMS), where the remote client works on the Telnet host machine as if it were a terminal attached directly to that host. Using Telnet, remote equipment, such as routers and switches, can be monitored and configured or remote systems can be operated as needed. Despite a primitive, character-oriented interface, Telnet remains one of the most important IP services.



A 32-bit windowed version of Telnet is available as part of Windows XP. To learn more about this utility, launch Telnet (type `telnet` from a Start|Run command) and access its Help utility.

SMTP

Simple Mail Transfer Protocol (SMTP) is used to provide IP-based messaging services. Although it is not the only email protocol available in the IP environment, most experts regard SMTP as the basis for Internet e-mail.

SNMP

Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for network management. SNMP is an industry-standard protocol supported by most networking equipment manufacturers. SNMP can query collections of management data, called management information bases (MIBs), on networked devices. This permits management applications to use SNMP to poll devices on the network and obtain regular status updates about their operating conditions, network utilization, and quality of service.

In addition, SNMP supports a trap mechanism that permits networked devices to send a message to a management application when specific events or error conditions occur. This capability is quite important because it permits networked devices to report potential or actual problems as soon as they are detected, rather than waiting for a management application to poll the device.



SNMP services are not activated by default on Windows XP. To enable these services, use the Optional Networking Components command from the Advanced menu of the Network Connections interface.

The Berkeley R Utilities

Among the many enhancements added to the UNIX TCP/IP implementation present in the Berkeley Software Distribution (BSD) in the 1980s was a collection of IP-based network commands collectively known as the “R utilities,” where the *R* stands for remote. This includes such commands as **rsh (remote shell)**, which permits a user on one network host to access shell commands on another network host and **rexec (remote execution)**, which permits a user on one network host to execute a program remotely across the network on another network host. Windows XP Professional supports both of these R utilities from the client side, but cannot act as a rsh or rexec server to other machines elsewhere on the network.



To learn more about rsh and rexec, start a DOS window (Start | All Programs | Accessories | Command Prompt) and enter either `rsh ?` or `rexec ?` at the command prompt to access the help files for these command-line utilities.

PING

Packet Internet Groper (PING) is one of the most colorful acronyms in the TCP/IP utility box. PING is a command-line utility that uses the ICMP protocol to inquire if a designated host is reachable on the network. It also provides information about the round-trip time required to deliver a message to that machine and to receive a reply.

PING is a very useful utility that permits you to see if your own machine is properly attached to the network. You can PING yourself by entering the command `PING 127.0.0.1` or `PING loopback`; in the latter case, this special address is defined as the loopback address, or the address of your own machine. You can find out if the network

itself is working by pinging a nearby machine. Finally, you can determine if a particular machine is reachable by pinging either its host name or the equivalent numeric IP address. All of this capability comes in handy when installing and testing IP on a new machine or when you need to troubleshoot a network connection.



To learn more about PING, launch a DOS window (Start|All Programs|Accessories|Command Prompt) and enter PING (with no arguments) at the command prompt to access its online Help file. Note that PING can supply all kinds of routing and quality of service data, as well as simply test for reachability.

TFTP

Trivial File Transfer Protocol (TFTP) is a lightweight analog of FTP that uses UDP as its transport protocol rather than TCP. TFTP is a much more stripped-down version of file transfer services than FTP; all it basically supports is the ability to communicate with a TFTP server elsewhere on the network and to copy files from the workstation to a remote host, or vice versa. For directory navigation, file grooming, or format translations, FTP is a much better choice.



To learn more about TFTP, start a DOS window (Start|All Programs|Accessories|Command Prompt), and enter TFTP ? at the command prompt to view its online Help file.

The HOSTS File

The **HOSTS** file is a static file placed on members of a network to provide a resolution mechanism between host names and IP addresses. The HOSTS file was the name resolution used before DNS was created. HOSTS files are used on small networks where the deployment of a DNS server is unwarranted or for remote systems to reduce traffic over slow WAN links. HOSTS files can also be employed to hard-code important systems, such as mission-critical servers. Assigning a static IP address in this way prevents a DNS glitch from inhibiting access. Each line of a HOSTS file contains an IP address followed by one or more corresponding host names to that IP address. A system processes the HOSTS file on a line-by-line basis when attempting to resolve a host name. Once the first match is reached, the resolution process terminates and the acquired IP address is used. HOSTS files are only as useful as they are current. Most administrators update their HOSTS file on a regular basis and have a logon script automatically download the HOSTS file from a central location to remote systems each time they log onto the network.

Windows XP includes a sample HOSTS file in the %systemroot%\System32\drivers\etc folder. The HOSTS file is a plain text document that can be edited with Notepad or any other text editor. Basic information about editing the HOSTS file is included in its own header text, but for complete information please consult the *Microsoft Windows .NET Server Resource Kit* or a text on the TCP/IP Protocol.

DNS

Domain Name Service (DNS) is a critical component of the Internet's ability to span the globe. DNS handles the job of translating a symbolic name such as *lanw02.lanw.com* into a corresponding numeric IP address (172.16.1.7). It can also provide reverse lookup services to detect machines that are masquerading as other hosts. (A reverse lookup obtains the symbolic name that goes with an IP address; if the two do not match, some form of deception is at work.)

DNS is a powerful, highly distributed database that organizes IP names (which, for its purposes, must take the form of fully qualified domain names) into hierarchical domains. When a name resolution request occurs, all the DNS servers that can identify themselves to each cooperate very quickly to resolve the related address. DNS servers include sophisticated caching techniques that permit them to store recently requested name-address pairs, so that users can get to a previously accessed address quickly.



Windows XP Professional can communicate with DNS servers, but only Windows .NET Server supports a full-fledged DNS server implementation.

The LMHOSTS File

The **LMHOSTS** file is a static file placed on members of a network to provide a resolution mechanism between NetBIOS names and IP addresses. The LMHOSTS file was the name resolution used before WINS was created. Now LMHOSTS files are used only on small networks where the deployment of a WINS server is unwarranted, or for remote systems to reduce traffic over slow WAN links. Each line of an LMHOSTS file contains an IP address followed by the corresponding NetBIOS name. A system processes the LMHOSTS file on a line-by-line basis when attempting to resolve NetBIOS names. Once the first match is reached, the resolution process terminates and the acquired IP address is used. LMHOSTS files are only as useful as they are current. Thus, most administrators update their LMHOSTS file on a regular basis and have a logon script automatically download the LMHOSTS file from a central location to remote systems each time they log onto the network.

Windows XP includes a sample LMHOSTS file in the *%systemroot%\System32\drivers\etc* folder, which is named LMHOSTS.SAM. The LMHOSTS file is a plain text document that can be edited with Notepad or any other text editor. Basic information about editing the LMHOSTS file is included in its own header text, but for complete information consult the *Microsoft Windows .NET Server Resource Kit*.

WINS

Windows Internet Naming Service (WINS) is not a true native TCP/IP service; it is an extension added by Microsoft. As previously discussed, most of the internal and network communications within a Microsoft network employ NetBIOS. On a TCP/IP network, NetBIOS

names must be resolved into IP addresses so packets can be properly delivered to the intended recipient. This process is automated by the WINS service. WINS dynamically associates NetBIOS names with IP addresses and automatically updates its database of associations as systems enter and leave a network, so it does not require ongoing maintenance. WINS is the dynamic service that is used to replace the static mechanism of the LMHOSTS file.

IPCONFIG

IPCONFIG is used to manage and view information related to DHCP and DNS. When used alone without any parameters, IPCONFIG displays the IP address, subnet mask, and default gateway for all network interfaces on the local machine. The parameters and syntax of IPCONFIG are:

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]]
[/flushdns] [/displaydns] [/registerdns] [/showclassid
Adapter] [/setclassid Adapter [ClassID]]
```

- *all*—Shows all TCP/IP configuration details for all network interfaces.
- *renew [Adapter]*—Forces a renewal of the address lease with the DHCP server, without a specified *Adapter*, the renewal occurs on all DHCP configured network interfaces. The *Adapter* value should be replaced with a name listed when IPCONFIG is executed without parameters.
- *release [Adapter]*—Releases the address lease with the DHCP server, without a specified *Adapter*, the release occurs on all DHCP configured network interfaces. The *Adapter* value should be replaced with a name listed when IPCONFIG is executed without parameters.
- *flushdns*—Clears and resets the DNS client resolver cache. This parameter should be used to remove negative cache entries and dynamically added entries.
- *displaydns*—Shows the content of the DNS client resolver cache. The cache includes preloaded entries from the HOSTS file and any resource records still in memory from resolved queries. The cache is used to attempt to resolve new queries locally before contacting a DNS server.
- *registerdns*—Forces the system to register all local IP addresses and DNS names with DNS. This parameter should be used to replace a failed automatic DNS registration or resolve a dynamic update problem without needing to reboot. The data on the DNS tab of advanced TCP/IP settings determine the information sent to the DNS server for registration.
- *showclassid Adapter*—Shows the DHCP class ID for the specified adapter. An asterisk can be used to show DHCP class IDs for all adapters. The *Adapter* value should be replaced with a name listed when IPCONFIG is executed without parameters.

- *setclassid Adapter [ClassID]*—Sets the DHCP class ID for the specified adapter, if the ClassID parameter is provided. This parameter clears the DHCP class ID for the specified adapter, if the Class ID is not provided. An asterisk can be used to indicate all adapters. The *Adapter* value should be replaced with a name listed when IPCONFIG is executed without parameters.

Other TCP/IP Command Line Tools

There are a wide range of TCP/IP command line tools used for network connectivity analysis and troubleshooting. These include NETSTAT and NBTSTAT. NETSTAT displays a list of active TCP connections. This list includes open ports, Ethernet statistics, the IP routing table, and IPv4/IPv6 statistics. The parameters and syntax of NETSTAT are as follows:

```
Netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s]
[Interval]
```

- *a*—Shows a list of active TCP connections and open TCP and UDP ports.
- *e*—Shows Ethernet statistics, such as sent and received bytes, unicast packets, nonunicast packets, discards, errors, and unknown protocols. This parameter can be used with *-s*.
- *n*—Shows a list of active TCP connections using IP addresses and port numbers only, no human friendly names are given.
- *o*—Shows a list of active TCP connections and shows the process ID (PID) for the active process using the connection. The PID can be used to cross reference the actual process name on the Processes tab of the Task Manager. This parameter can be used with *-a*, *-n*, and *-p*.
- *p Protocol*—Lists the connections for the specified *Protocol*. The value of *Protocol* can be *tcp*, *udp*, *tcpv6*, or *updv6*. If this parameter is used with *-s*, the value of *Protocol* can be *tcp*, *udp*, *tcpv6*, *updv6*, *icmp*, *ip*, *icmpv6*, or *ipv6*.
- *r*—Shows the IP routing table. This parameter displays the same information as the *route print* command.
- *s*—Lists statistics by protocol. By default, it only displays information for TCP, UDP, ICMP, and IP. If IPv6 is installed, then the displayed statistics will be for the v6 version of these protocols. This parameter can be used with *-p*.
- *Interval*—Configures the system to redisplay the selected information every *Interval* seconds with updated information. CTRL+C terminates the repeated display of data. If this parameter is not used, *netstat* displays the requested information only once.

NBTSTAT displays protocol statistics for NetBIOS over TCP/IP (NetBT), NetBIOS name tables, and the NetBIOS name cache. NBTSTAT can also be used to force a

refresh of the NetBIOS name cache and names registered with WINS. The parameters and syntax of NBTSTAT are (the parameters of NBTSTAT are case-sensitive):

```
Nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
```

- *a RemoteName*—Shows the NetBIOS name table on a remote computer indicated by the NetBIOS computer name *RemoteName*.
- *a IPAddress*—Shows the NetBIOS name table on a remote computer indicated by the *IPAddress*.
- *c*—Shows the contents of the NetBIOS name cache table of the local system and related IP addresses.
- *n*—Shows the NetBIOS name table of the local system.
- *r*—Shows NetBIOS names resolution and registration statistics.
- *R*—Clears the NetBIOS name cache and rebuilds it by loading the #PRE entries from the LMHOSTS file.
- *RR*—Clears and refreshes the NetBIOS names for the local system which are registered with WINS.
- *s*—Shows information about NetBIOS connections, such as client and server sessions. Remote hosts are resolved into NetBIOS names when possible.
- *S*—Shows information about NetBIOS connections, such as client and server sessions. Remote hosts are displayed only as IP addresses.
- *Interval*—Configures the system to redisplay the selected information every *Interval* seconds with updated information. CTRL+C terminates the repeated display of data. If this parameter is not used, NBTSTAT displays the requested information only once.

TCP/IP CONFIGURATION

TCP/IP configuration is performed through the Network Connections interface. When configuring TCP/IP for Windows XP Professional, there are many items of information that you need. If the machine uses DHCP, the DHCP server handles all these details. If not, here's a list of items that you might need to obtain from a network administrator (or figure out for yourself, if that's your job):

- A unique IP address for the computer
- The subnet mask for the network to which the computer belongs
- The address of the default gateway, the machine that attempts to forward any IP traffic not aimed at the local subnet (which makes it the gateway to other networks)

- The address of one or more DNS servers, to provide IP name resolution services. This is more important on bigger networks than on smaller ones. If you use an ISP for network access, you'll probably need to get this address from them
- On Windows-based networks in particular, you might need to provide an address for a WINS server, which permits NetBIOS name resolution requests to be transported across IP networks (even through routers if necessary)

When TCP/IP is installed, its default settings are to seek out a DHCP server to provide all configuration settings. If a DHCP server is already present on your network, you do not need to configure TCP/IP to be able to access the network. When an interface is configured to use DHCP, an additional tab, called Alternate Configuration, is revealed. This tab is used to define a set of TCP/IP configurations that can be used in the event that DHCP communication fails. If an alternate configuration isn't manually defined, Windows XP automatically assigns a configuration via APIPA (Automatic Private IP Addressing). This automatic configuration will have an IP address within the range of 169.254.0.1 through 169.254.255.254 and a subnet mask of 255.255.0.0.

TCP/IP configuration takes place in the Internet Protocol (TCP/IP) Properties dialog box. (Refer to Figure 7-5.) Access the dialog box by clicking the Properties button after selecting TCP/IP from the list of installed components from the Properties dialog box of a Local Area Connection from the Network Connections interface. On a multihomed system (a computer with more than one network interface card) the configuration for each adapter can be different. Be sure to select the correct Local Area Connection object for the adapter you want to modify.

There are two ways to assign an IP address to a computer: manually or through DHCP. As discussed earlier, DHCP is used to automatically configure the TCP/IP settings for a computer. If a DHCP server is available and will be used to configure this computer, select the Obtain an IP address automatically option. If there is no DHCP server available or if the configuration is to be handled manually, select the Use the following IP address option.

Before you can do this, you must obtain a valid IP address from a network administrator or your ISP. If your network does not need to access the Internet directly (or address translation software mediates Internet access on your behalf), you can assign private IP addresses from a number of reserved address ranges that the InterNIC has set aside for this purpose. To learn more about these private address ranges and how to use them, download a copy of RFC 1918 at <http://www.cis.ohio-state.edu/rfc/rfc1918.txt>.

If you select Specify an IP address, the remaining three boxes become active. When you are finished, the IP Address box should display the correct IP address for that computer.



If you are entering an IP address into an entry box, press the period key to jump from one octet to the next. This comes in handy when an address does not contain a three-digit number in any octet field. You can also use the right arrow key to advance the cursor, but don't use the Tab key—it advances the cursor to the next input field and forces you to backtrack to complete the IP address specification.

As described earlier, the subnet mask defines which part of the IP address represents the network and which part represents the host. You must supply this information or your computer will not be able to communicate using TCP/IP.

The default gateway for a computer specifies the host, usually a router, to which the computer should send data that is not destined for the computer's subnet. For example, if a computer's address is 156.24.99.10 with a subnet mask of 255.255.255.0, its host address is 10 and its network address is 156.24.99. If this computer had data to send to a computer whose address was 203.15.13.69, it sends the packets to the default gateway for forwarding to the appropriate network. Whenever connectivity to other networks is required, you must provide an IP address for the default gateway on the machine's network segment. If you don't, traffic from your machine will not be able to get to machines that are not on the same network segment as your computer.

Clicking the Advanced button opens the window shown in Figure 7-7. The IP Addresses area allows you to assign multiple addresses to one network adapter, whereas the Gateways area provides support for multiple router configurations.

By selecting the DNS tab, shown in Figure 7-8, the user is able to configure DNS on his or her computer. Multiple DNS servers can be defined along with setting their use priority. You can also define how incomplete domain names or host names are resolved (e.g., by adding suffixes to create a fully qualified domain name).

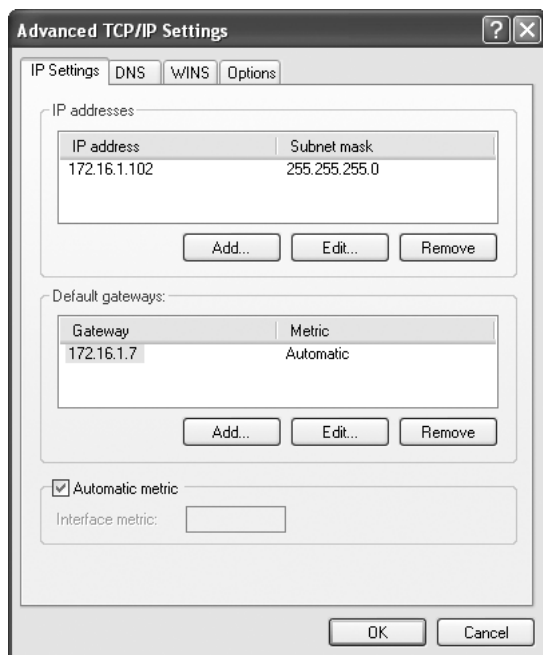


Figure 7-7 The Advanced TCP/IP Settings dialog box, IP Settings tab

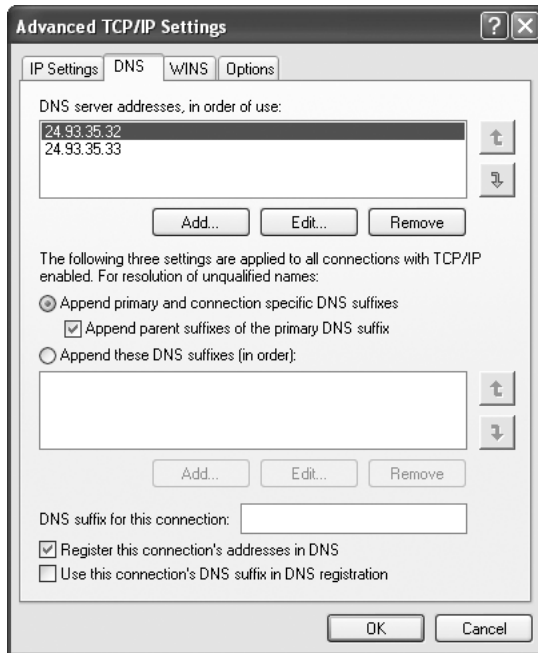


Figure 7-8 The Advanced TCP/IP Settings dialog box, IP DNS tab

Use the WINS tab (see Figure 7-9) to configure WINS settings. You can define multiple WINS servers and set their use priority. You can also enable or disable the use of an LMHOSTS file. Furthermore, you can enable, disable, or save the setting to the DHCP server whether or not this system will use NetBIOS over TCP/IP.

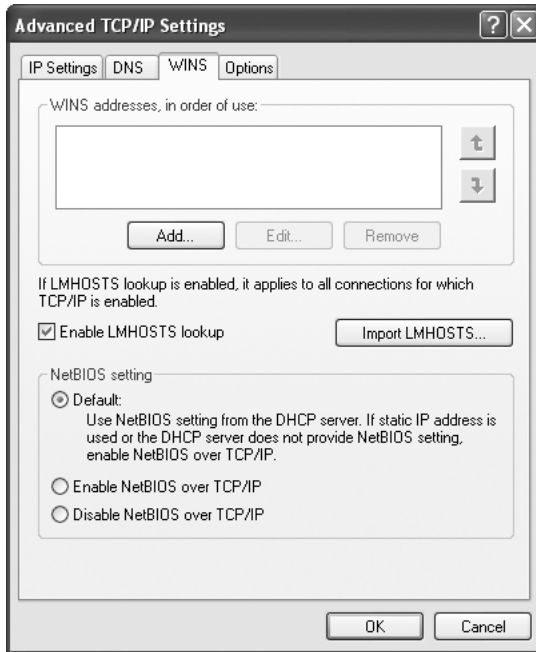


Figure 7-9 The Advanced TCP/IP Settings dialog box, WINS tab

The Options tab lists optional TCP/IP-related services or capabilities. The two default optional items are IP Security and TCP/IP filtering. Selecting a listed item and clicking Properties reveals a service-specific configuration dialog box. IPsec is briefly discussed in Chapter 6, “Windows XP Security and Access Controls.” For more information about configuring these and other optional items, consult the *Microsoft Windows .NET Server Resource Kit*.

IPv6: LOOKING TO THE FUTURE

Over the last several years, researchers have endeavored to update and improve TCP/IP. Of primary importance is the number of available addresses. When TCP/IP was developed using a 32-bit address space, nobody conceived that there could ever be an address shortage. It seemed that over four billion addresses would be enough. This proved to be wrong. IPv6 aims to correct the address shortage and improve other aspects of TCP/IP, including security and efficiency. IPv6 uses a 128-bit address space, which results in over 3.4×10^{38} (340,000,000,000,000,000,000,000,000,000,000) addresses.

Microsoft has included preliminary support for IPv6 in Windows XP. This support includes socket extensions and updated RPC systems to handle the 128-bit addresses. Microsoft also included a Developers Edition of the IPv6 protocol, which should be used only for research and testing purposes. Once IPv6 has been finalized, Microsoft will

most likely include an IPv6 upgrade in a service pack or other downloadable installation module.

For more information about IPv6, consult the Help and Support Center on the Microsoft Web site. At the time of this writing there were at least three useful resources: <http://www.ipv6.org>, <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/namead-rmgmt/introipv6.asp>, and <http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp>. However, if these documents are moved, you can always perform a search using IPv6 as the keyword.

WINDOWS XP REMOTE TOOLS

Microsoft has aimed to improve remote access to client systems over networks and the Internet. This is evident in two new features: Remote Assistance and Remote Desktop. Remote Assistance allows a distant user to view your desktop and even have control over the mouse and keyboard activities. Remote Desktop enables you to access your client's logon environment from a remote system.

Both of these remote tools are enabled on the Remote tab of the System applet. Once Remote Assistance is enabled, you can also set whether this system can be fully controlled remotely and the maximum lifetime of invitations. Once Remote Desktop is enabled, you can define which users can establish a remote connection.

Remote Assistance

Remote Assistance was designed to simplify the task of training users or walking users through tasks. An administrator or trainer can remotely show the end user the steps required to perform some function right on the user's system. Remote Assistance even supports real-time two-way chat (text or voice) between the end user and the remote assistant.

To simplify the discussion of this feature, let's label the end-user who needs assistance as the student and the person who will remotely provide help the teacher. When a student wants help through Remote Assistance, he or she must send out an invitation to the teacher from whom they need help. This is done using Windows Messenger or by e-mailing an invitation script to the teacher. It is even possible to save the invitation to a file (named `rcBuddy.MsRcIncident`) and use some other means to send it to the teacher. To initiate a Remote Assistance invitation, use the Invite a friend to connect to your computer with Remote Assistance link from within Help and Support. Remote Assistance invitations have an expiration time limit, which you define when sending the invitation. Invitations also can have a password associated with them to prevent unwanted persons from using the invitation to gain access to your system.

Once connected, both participants can chat, exchange files, or disconnect the session. The teacher can take full control of the student's system to demonstrate an activity or perform some action. Remote Assistance is an excellent tool for training and troubleshooting.

Both systems must be Windows XP or newer with either Windows Messenger Service or a MAPI-compliant e-mail utility (such as Microsoft Outlook or Outlook Express). Both systems must be able to communicate with each other over a network connection and have Internet access. The faster the connectivity between the two systems, the more responsive the control will be. Remote Assistance can be used to link two systems on the same LAN or two systems anywhere in the world over the Internet.

For more information on Remote Assistance, see the Help and Support Center as well as the *Microsoft Windows .NET Server Resource Kit*.

Remote Desktop

Remote Desktop is similar to a single client Terminal Services for clients. Remote Desktop was developed so workers can access their work desktops (a.k.a. host client) from their home systems (a.k.a. remote system). Through Remote Desktop, you have the same access to your files and applications as you do when you are physically sitting at the system.

Remote Desktop is enabled through a component of IIS, namely Remote Desktop Web Connection. This component need only be installed on the IIS server on the same network as the client, not necessarily on the client itself. Once properly configured, you need to switch away from your desktop on the host client. Then, from the remote system, open `http://<servername>/tsweb/` in Internet Explorer, where `<servername>` is the IIS server, then provide the IP address or name of the host client. Once connected, you'll have full control over the host client, just as if you were seated at its keyboard.

A second method to support Remote Desktop connections does not directly involve IIS. The Remote Desktop Connection utility can be installed on a Windows 9x, NT, or 2000 system directly from the Windows XP distribution CD. The Remote Desktop Connection allows a link between a remote system and the client without the need of IIS.

For more information on Remote Desktop, see the Help and Support Center as well as the *Microsoft Windows .NET Server Resource Kit*.

WINDOWS XP AND NETWARE NETWORKS

Novell NetWare is designed for file and printer sharing on a network. Because it was one of the first true network operating systems, NetWare garnered a substantial and loyal following throughout the late 1980s and early 1990s. By the mid-1990s, NetWare servers functioned as the backbone for more networks than any other type of server on the market. The most recent iteration of NetWare is NetWare 6. With the growth of PC capabilities and the advent of the Internet, NetWare has adapted and expanded to provide robust services, while maintaining its solid file and printer sharing performance.

Although servers running Windows NT, Windows 2000, or other versions of Windows account for a growing number of network servers, a large number of companies around

the world rely on Novell NetWare for their server requirements. For this reason, Microsoft includes interconnectivity enhancements to allow Windows XP-based computers to connect to and function with NetWare servers. These enhancements include NWLink, Client Service for NetWare, File and Print Services for NetWare, and Gateway Services for NetWare. Of these, only NWLink and Client Service for NetWare are used by Windows XP Professional systems. File and Print Services for NetWare and Gateway Services for NetWare are used by Windows Server computers, not on end-user workstation computers.

Beginning with version 1.0, NetWare utilized a datastore called the **bindery**, a proprietary database that contains network resource information, such as user and group names, print server settings, and file server configurations. With NetWare 4.0, Novell introduced **Novell Directory Services (NDS)**. NDS is a hierarchical database used by NetWare 4.0 and newer servers to store network resource and object data, comparable in function to Active Directory in Windows 2000 and newer versions. With this introduction, Novell began the era of object-oriented directory services. In this context, a directory is a dynamic database that contains information for network objects such as printers, applications, and groups. Later sections of this chapter discuss the differences between connecting to bindery (pre-version 4.0) servers and NDS servers.

Because the Professional edition of Windows XP is designed to operate as a network client, it includes features that enable it to connect to a variety of network servers, including NetWare servers. Because both bindery and NDS servers remain in use today, Windows XP is able to connect to both types. Once connected, the Windows XP Professional computer utilizes resources on the NetWare server as if they were actually on a Windows server. In this way, all network resources are accessed using the same methods, thereby making a heterogeneous network appear seamless to its users.

NETWARE COMPATIBILITY COMPONENTS

There are two main components that facilitate Windows XP Professional compatibility with NetWare servers: NWLink and Client Service for NetWare. The next sections discuss installing and configuring these components.

NWLink

NWLink is Microsoft's implementation of the IPX/SPX protocol suite and can communicate with all NetWare implementations. Novell and Microsoft approach networking in different ways, meaning that the underlying architecture of each company's network access differs. Novell's specification is called the Open Datalink Interface (ODI). Microsoft's architecture is called the Network Device Interface Specification (NDIS). Strictly speaking, IPX/SPX is ODI-compliant, but not NDIS-compliant. NWLink is the NDIS-compliant implementation of IPX/SPX.

IPX (Internetwork Packet Exchange) is a connectionless protocol that provides quick network transport for most communications on a NetWare network. Because it is connectionless, IPX does not guarantee packet delivery, but it is generally sufficient for network communications. **SPX** (Sequenced Packet Exchange) is a connection-oriented protocol that provides guaranteed packet delivery. However, because it is connection-oriented, it requires higher overhead and is slower than IPX. For this reason, SPX is used in NetWare communications for only certain applications, such as those that manage the server's console.

Installing NWLink

Like all networking components in Windows XP, NWLink is installed through a connection object within Network Connections. From the Connect To entry, select the Show all Connections entry in the pull-out menu. Then, you can either right-click the connection to which you want to add NWLink and select the Properties entry from the pop-up menu, or double-click that connection and click the Properties button to produce the same window. Either way, you'll use the Install button to add the NWLink protocol. The Local Area Connection Properties window, shown earlier in Figure 7-4, shows information about the LAN connection on a test machine; note the Install button to the lower right of the connection items pane.

The Connection Properties window is where you add networking components to Windows XP. If the Typical installation option is selected during the installation process, Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks, the QoS (Quality of Service) Packet Scheduler, and Internet Protocol (TCP/IP) are loaded by default.

To connect to an older NetWare network, the NWLink protocol must be loaded (newer versions of NetWare—5.x or newer—use TCP/IP by default, and probably won't need this protocol). To add a new networking component to the Local Area Connection, click the Install button. You are presented with the Select Network Component Type dialog box, which allows you to install a client, service, or protocol. (Complete steps for installing NWLink appear in Hands-on Project 7-7.)

Configuring NWLink: Ethernet Frame Types and IPX Network Numbers

After installation is complete, NWLink has three configuration options available: Internal Network Number, Ethernet frame types, and network numbers. Ethernet can utilize four frame types supported by NWLink: Ethernet 802.2, Ethernet 802.3, Ethernet II, and Ethernet SNAP. A packet's frame type defines the structure of the packet and the fields that are included.

- **Ethernet 802.3**—Ethernet 802.3, also known as raw 802.3, is a Novell proprietary Ethernet frame format that Novell implemented prior to the completion of the 802.3 committee's frame format definition efforts. It served as the initial Ethernet frame scheme that Novell used, but seldom appears on networks today. It includes an Institute of Electrical and Electronic Engineers (IEEE) 802.3 Length field but not an IEEE 802.2 (LLC) header. The IPX header immediately follows the 802.3 Length field.

- **Ethernet 802.2**—802.3 is the standard IEEE 802.3 frame format which includes the IEEE 802.2 (LLC) header.
- **Ethernet II**—Ethernet Version 2 includes the standard Ethernet Version 2 header, which consists of Destination and Source Address fields followed by an EtherType field.
- **Ethernet SNAP**—SNAP extends the IEEE 802.2 header by providing a type code similar to that defined in the Ethernet Version 2 specification.



It is very important for all computers communicating on the network to use the same frame type to ensure that communication takes place. If frame types do not match, communication is not possible.

By default, Windows XP determines the frame type in use on the network and configures itself accordingly. It does this by accepting the first NWLink packet it receives and using the same frame type. If all computers on the network are set to Auto Detect, the Ethernet 802.2 frame type is used because it is the accepted industry standard for NWLink.

Unless there is a specific reason to use some different frame type, it's best to let Windows XP detect the frame type in use on the network. By doing so, potential problems caused by frame type mismatches are eliminated. However, if it is necessary to specify a frame type for the connection, select the appropriate frame from the Frame type drop-down list in the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol Properties dialog box. When a frame type other than Auto Detect is selected, you must specify an **IPX network number** (the network identifier) that the frame type uses (if you don't know this information, you'll need to get it from your network administrator).

Like TCP/IP, NWLink (IPX) makes a distinction between the computer ID and the network ID on which the connection resides. However, unlike TCP/IP, the computer ID and network ID, or network number, are separate fields in IPX. When the computer is configured to detect the frame type used on the network automatically, it is also able to determine the network number from the frames it receives. However, when a specific frame type is selected, you must also specify the network number to which the computer is attached. If the network number does not match the network number used by other computers on the network, your system will not be able to communicate.



Network numbers on IPX networks are not limited to numerals. Because the IP v4 and IPX addresses are both 32 bits long, IPX administrators can convert IP addresses to hexadecimal notation and use corresponding IP and IPX addresses for the same cable segments. For example, the Class C IP address 192.168.1.0 converts to C0A80100, 192.168.2.0 converts to C0A80200, and so on, for the various logical networks that might occur on a corporate LAN.

Part of the design of IPX utilizes a network number assigned to the internal operations of the computer. Under most circumstances, it is not necessary to change this number. However, if the network number that is assigned to the internal network number is in use elsewhere on the network as a normal network number, communication will be sporadic and difficult to troubleshoot.

Client Service for NetWare

The Client Service for NetWare (CSNW) component of Windows XP Professional allows a Windows XP computer to access resources on NetWare servers version 2x, 3x, and 4x. CSNW supports full access to NetWare file and print servers, NetWare utilities, bindery connections, and some NDS connections.



The version of CSNW that is included with Windows XP Professional is not compatible with all features of the NetWare 6.x version of NDS. CSNW allows authentication to NetWare 5.0 NDS-enabled servers, but for full functionality, load the 32-bit Windows client software provided with NetWare.

File and Print Servers

To provide access to NetWare file and print servers, CSNW adds a NetWare-focused redirector that acts as an extension of the file system, in much the same way that the native redirector supports access to Microsoft Windows Servers. (Redirectors handle transmission of remote requests across the network so that the requests are filled.) The difference is that CSNW implements **NetWare Core Protocol (NCP)** requests for file and print services, whereas the native redirector uses the **Common Internet File System (CIFS)**, an enhanced version of the Server Message Block (SMB) protocol. Both NCP and SMB perform the same functions, but provide access to different file systems.

Once CSNW is installed, a Windows XP user can use a single logon to access all resources on the network, regardless of the server hosting the resources. In a NetWare-only environment, only CSNW is active and it provides access to resources. However, in a mixed NetWare/Windows server environment, the appropriate client software is used, depending on the type of server being accessed. (Installation of CSNW is covered in a later section; complete steps are given in Hands-on Project 7-9.)

Supported NetWare Utilities

To ensure proper desktop integration in a NetWare server environment, CSNW supports most NetWare utilities and functions. It provides access to character-based NetWare administration utilities such as SYSCON and PCONSOLE. Many of the utilities are dependent on the versions of NetWare in use. Versions 3.12 and lower support only character-based applications, whereas versions 4.0 and above utilize mainly GUI-based applications. However, even in NetWare 6, certain character-based utilities can be used to manage the server environment.



By default, NetWare versions before 5.0 do not support long filenames. To ensure that long Windows filenames are not truncated when they are copied to NetWare servers, those servers must load the OS/2 name space. This is done on the NetWare server itself and ensures that all files retain their settings when stored on the server.

NWLink and CSNW also support IPX burst mode, which enhances bulk data transfer over an IPX network. By design, IPX is best suited to handle small- to medium-sized packets and numerous network communications. When tasked with transferring large amounts of data, IPX loses efficiency and creates excessive network traffic. Burst mode allows routed network connections to negotiate the largest possible packet size so that fewer packets are sent to transmit large data files. This improves bandwidth utilization and reduces network overhead.

Bindery and NDS Support

To effectively ensure that client computers can attach to any server on the network, Client Service for NetWare includes support for both bindery and NDS servers. As mentioned, versions of NetWare prior to 4.0 used the bindery to store their configuration information, including user and group lists, printers, and security settings. When users logon to a bindery-based NetWare server, they access the bindery for logon authentication, confirmation of security authorizations, group memberships, and so forth. One of the primary limitations of bindery-based NetWare is that each server on the network has its own bindery. Users that access resources on multiple servers are required to logon to each server individually.

NetWare 4.0 uses a Novell Directory Services (NDS) database to store and maintain information that was previously stored in the bindery. The NDS database is much more dynamic and supports enterprise-wide networks. The NDS database is a hierarchical tree stored on many servers on the network that provides single-logon access to resources. In addition, centralized administration and resource management is possible with NDS—a real improvement over earlier versions of NetWare.

Because NDS is a hierarchical database that can be stored on multiple servers on the network, an NDS implementation resembles a tree and is referred to as the **NDS tree**. At the base of the tree is the Root object, which generally represents the largest organization connected to the network, often the entire corporation. Working down through the tree, each department may have a container, then each group within the department can have another container. In NDS, each network resource, whether a user, group, file server, printer, or storage area, is represented as an object. Objects are stored in containers representing their function on the network. A network object's location in the NDS tree is called its **context**. Figure 7-10 is an example of an NDS tree.

In the example shown in Figure 7-10, the Phillip user object resides in the Sales container, which in turn resides in the Sales/Marketing container, which resides under the DJNet Enterprises Root object. The context for the Phillip user is DJNet Enterprises.Sales/Marketing.Sales.

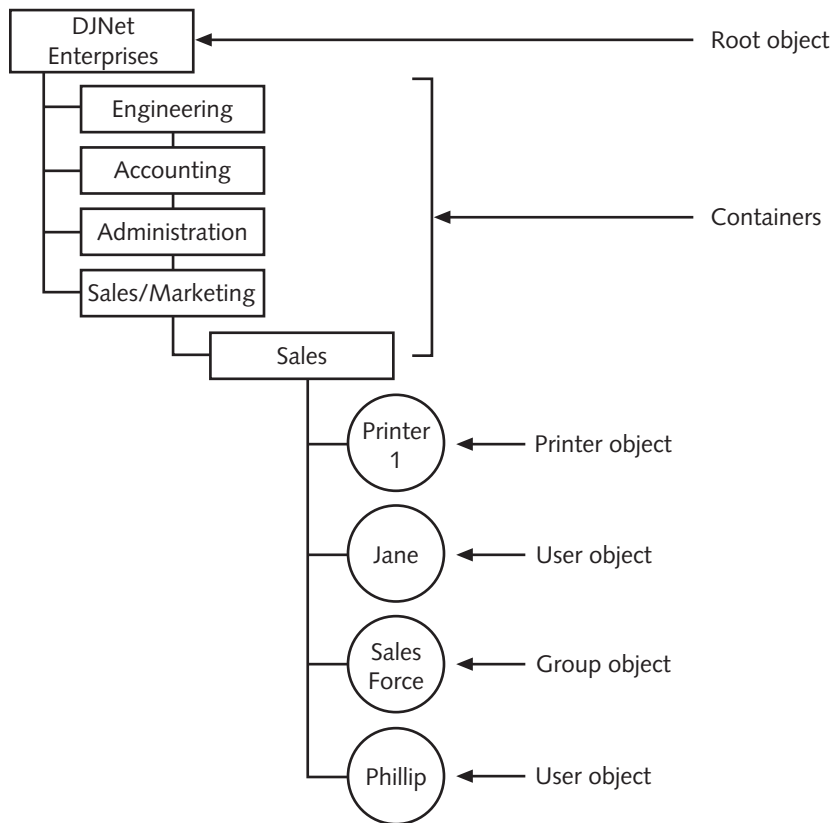


Figure 7-10 Illustration of an NDS tree structure

Installing and Configuring Client Service for NetWare

Like NWLink, installation of Client Service for NetWare occurs in the Local Area Connection Properties dialog box. Once in that window for the appropriate connection object, click **Install**; you will be asked whether to install a **Client**, **Service**, or **Protocol**. As its name implies, Client Service for NetWare is a client component. Select **Client** and click **Add**. If the default configuration is installed, the only client available for installation is CSNW. Ensure that Client Service for NetWare is selected and click **OK** to continue the installation. Once installation is complete, you will be asked to restart your computer. You must do so before CSNW can be used. Click **Yes** to reboot your computer.



Client Service for NetWare relies on NWLink to operate. If NWLink is not loaded when CSNW is installed, it will be installed automatically.

Assigning a Default Tree and Context Using CSNW

After the computer has restarted, you will be presented with the Select NetWare Logon dialog box. It is through this dialog box that you assign a default NetWare tree and context on the NDS-enabled NetWare network to which the Windows XP Professional computer will connect. Unlike most areas of Windows XP, you cannot browse for tree and context data. You must have this information available to type into the dialog box. If this information is not available the first time the computer is restarted, you can click Cancel and enter the information later.

Unlike many networking components, CSNW is not configured through the Local Area Connection Properties dialog box. When CSNW is installed, a separate utility is placed in the Control Panel, and represented by the CSNW icon. If at any point you need to change the default tree and context settings, or any CSNW settings, double-click the CSNW icon to access the Client Service for NetWare configuration dialog box. When accessed by this method, additional configuration options are available, as discussed in later sections.



The CSNW applet appears in the Control Panel only in Classic View; it is not available in Category View.

Preferred Server vs. Directory Tree

Should you need to connect a Windows XP Professional computer to a bindery-based NetWare server, you must use the Preferred Server configuration options available in the Client Service for NetWare applet (see Figure 7-11). Unlike the Default Tree and Context settings where you must type in the tree and context manually, clicking the down arrow next to the Preferred Server box displays a list of all servers that advertise themselves on your network. From that list, select the name of the NetWare server to which you want to attach. You can also enter the server's name in the Preferred Server box directly. If making a manual entry, be sure the server's name is spelled correctly. If an incorrect server name is entered, the dialog box shown in Figure 7-12 appears, informing you that you could not be authenticated on the selected server because the network path could not be found. Clicking No returns you to the Select NetWare Logon dialog box, whereas clicking Yes accepts the configuration anyway.

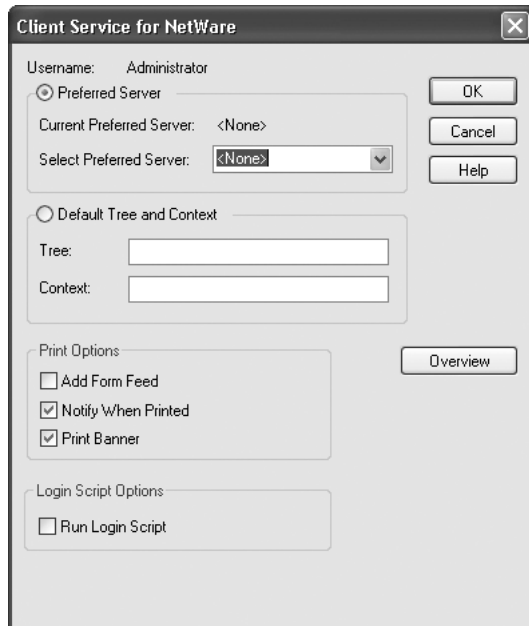


Figure 7-11 The Client Service for NetWare applet



Figure 7-12 Client Service for NetWare error (incorrect server path)

Regardless of the configuration changes you make, a dialog box is invoked notifying you that the changes will take effect the next time you log in. Click OK to continue. The computer must be restarted manually, because the configuration program does not automatically restart the computer after the dialog box is closed.

Other Configuration Settings

When you use the Client Service for NetWare applet to configure networking components, configuration options are available that are not presented when the client is first installed. As shown in Figure 7-11, these options make up the bottom half of the dialog box, in the Print Options and Login Script Options section.

The settings available in the Print Options section determine whether a computer sends a form feed command to the printer when the print job is finished, sends a notification message to the user when the print job is complete, or prints a banner before the print

job itself. Form feed commands are generally necessary only on older printers, usually those that use tractor-feed paper; most laser and inkjet printers do not require form feed commands to end a print job. If this option is used on a laser printer, for example, a blank sheet of paper is ejected from the printer after the job. Many users in a networked environment are not within eyesight of the printers they are using. For that reason, the Client Service for NetWare can be configured to send a network notification to the user after a job is complete. If that option is selected, a pop-up box appears on the user's computer when the print job is done. The banner page is also used in many larger networks. A banner page identifies the user who initiated the print job and the name of the job. Thus, users can easily identify their print jobs when they go to pick them up from the printer.

When the Run Login Script option is selected, the computer runs the NetWare logon script specified for the user by the administrator. This preserves logon scripts that network administrators have developed for their clients and provides easy, centralized administration for all client computers. This is especially important to standardize client behavior, regardless of the client type. However, many of the functions that logon scripts provide also work using Windows XP functions such as Map Network Drive. As more client computers are converted to Windows XP Professional, it may no longer be necessary to use logon scripts, and this option can be disabled.



Note that Novell uses the terms "log in" and "login," whereas Microsoft uses "log on" and "logon."

CONNECTING TO NETWARE RESOURCES

Because Client Service for NetWare integrates so closely with Windows XP, connecting to NetWare resources works the same way as connecting to other resources. Most often, this is accomplished through My Network Places. In an NDS environment, if the resources to which you are connecting are in the same NDS tree, your initial logon provides you access to available resources. However, on bindery-based networks, you must logon to each server to access the resources on that server. Once you have logged on to the appropriate server or directory tree, the NetWare security system determines whether you should be granted access to the requested resources.

Through the Computers Near Me icon in My Network Places, you can connect to resources on servers or trees to which you have already logged on. To search for other servers or NDS trees, double-click the Entire Network icon, and click the Entire Contents link shown in the lower-left corner.

After clicking on the link, you will be presented with icons for each type of client installed, usually Microsoft Windows Network and NetWare or Compatible Network. To browse for additional NetWare resources, double-click the NetWare or Compatible Network icon.

Choosing Appropriate NetWare Client Software

Because Novell also offers its Novell 32-bit Client for Windows, you may sometimes find yourself forced to choose between the Windows Client for NetWare Networks or the Novell equivalent when setting up Windows XP Professional workstations for network access. In that case, we urge you to consider the following list of factors to help you choose an appropriate client:

- On networks where NetWare servers outnumber Windows servers, or where clients need native NDS or NetWare-aware applications support, it's sensible to use the Novell 32-bit client for Windows.
- On networks where Windows servers outnumber NetWare servers, or where clients need native Active Directory and Windows applications support, it may make more sense to use the Microsoft Client for NetWare networks.
- In situations where an equal number of servers of each type occur, or where NDS or NetWare-aware applications aren't necessary, it's far easier to install and use the Microsoft Client for NetWare networks.
- When all that's required for Windows XP clients is access to file and print services on NetWare servers, you may want to consider installing Gateway Services for NetWare on Windows servers, because they can mediate access to NetWare file and print services. In that case, no NetWare client software of any kind is needed.

If you let your circumstances dictate the choice of client, remember also the principle of “least administrative effort.” This means that you should evaluate which approach involves the least amount of effort to implement, and weigh its pros and cons very carefully. Only when the balance firmly tilts toward the cons should you consider a different implementation approach!



If you decide to install the Novell 32-bit Windows client, you may not also install NWLink or CSNW (in fact, if you've installed those Microsoft components, you must first uninstall them before you attempt to install the Novell components).

CHAPTER SUMMARY

- Windows XP Professional provides network access primarily by using TCP/IP. TCP/IP is routable, supports enterprise-level networks, and has been designed to interconnect dissimilar types of computers, which helps to explain why it's the protocol of choice on the Internet. TCP/IP is an industry-standard protocol that provides easy cross-platform communication.

- Windows XP includes a number of applications that utilize TCP/IP and provide Internet connectivity. In spite of TCP/IP's complexity, configuring Windows XP to employ this protocol is not difficult.
- Windows XP includes several new networking features and utilities; these include network bridging, Remote Assistance, Remote Desktop, greater support for wireless networking, and support for the upcoming IPv6 protocol.
- Windows XP includes the NWLink protocol and Client Service for NetWare (CSNW) to enable users to access resources and services from NetWare-based networks. This implementation supports older, bindery-based NetWare servers (3.x and older) as well as newer, Novell Directory Services-based NetWare servers (4.x and newer).
- When choosing NetWare client software for use on Windows XP clients, pick the client that fits the majority of servers in use, or that provides native support for the most important directory and application services.

KEY TERMS

Address Resolution Protocol (ARP) — The IP protocol used to resolve numeric IP addresses into their MAC layer physical address equivalents.

bindery — The database used by versions of NetWare before 4.0 to store network resource configuration information.

binding — The process of developing a stack by linking together network services and protocols. The binding facility allows users to define exactly how network services operate for optimal network performance.

Client Service for NetWare (CSNW) — Service included with Windows XP Professional that provides easy connection to NetWare servers.

Common Internet File System (CIFS) — An enhanced version of SMB used for file and print services.

connectionless — A class of network transport protocols that makes only a “best-effort” attempt at delivery, and that includes no explicit mechanisms to guarantee delivery or data integrity. Because such protocols need not be particularly reliable, they are often much faster and require less overhead than connection-oriented protocols.

connection-oriented — A class of network transport protocols that includes guaranteed delivery, explicit acknowledgement of data receipt, and a variety of data integrity checks to ensure reliable transmission and reception of data across a network. Although reliable, connection-oriented protocols can be slow because of the overhead and extra communication.

context — The location of an NDS object in the NDS tree.

Data Link Control (DLC) — A network transport protocol that allows connectivity to mainframes, printers, and servers running Remote Program Load software.

Domain Name Service (DNS) — TCP/IP service that is used to resolve names to IP addresses.

Dynamic Data Exchange (DDE) — A method of interprocess communication within the Windows operating system.

Dynamic Host Configuration Protocol (DHCP) — An IP-based address management service that permits clients to obtain IP addresses from a DHCP server. This allows network administrators to control and manage IP addresses centrally, rather than on a per-machine basis.

File Transfer Protocol (FTP) — The protocol and service that provides TCP/IP-based file transfer to and from remote hosts and confers the ability to navigate and operate within remote file systems.

frame type — One of four available packet structures supported by IPX/SPX and NWLink. The four frame types supported are Ethernet 802.2, Ethernet 802.3, Ethernet II, and Ethernet SNAP.

HOSTS — A static file placed on members of a network to provide a resolution mechanism between host names and IP addresses.

Internet Control Message Protocol (ICMP) — The protocol in the TCP/IP suite that handles communication between devices about network traffic, quality of service, and requests for specific acknowledgments (such as those used in the PING utility).

Internetwork Packet Exchange (IPX) — The protocol developed by Novell for its NetWare product. IPX is a routable, connection-oriented protocol similar to TCP/IP but much easier to manage and with lower communication overhead.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — The name of the two primary protocols developed by Novell for its NetWare network operating system. IPX/SPX is derived from the XNS protocol stack and leans heavily on XNS architecture and functionality. See also IPX and SPX.

Internet Protocol (IP) — The protocol that handles routing and addressing information for the TCP/IP protocol suite. IP provides a simple connectionless transmission that relies on higher layer protocols to establish reliability.

interprocess communication (IPC) — The mechanism that defines a way for internal Windows processes to exchange information.

LMHOSTS — File is used in Microsoft networks to provide NetBIOS name-to-address resolution.

mailslots — A connectionless version of named pipes; mailslots offer no delivery guarantees, nor do they acknowledge successful receipt of data.

Multiple Universal Naming Convention Provider (MUP) — A Windows XP software component that allows two or more UNC providers (for example, Microsoft networks and NetWare networks) to exist simultaneously. The MUP determines which UNC provider will handle a particular UNC request and forwards the request to that provider.

Multi-Provider Router (MPR) — A file system service that can designate the proper redirector to handle a resource request that does not use UNC naming. The MPR lets applications written to older Microsoft specifications behave as if they used UNC naming. The MPR is able to recognize those UNC names that correspond to defined drive mappings receive copies of the domain security database or Active Directory.

- named pipes** — Provides support for a connection-oriented message passing service for clients and servers.
- NDS tree** — The hierarchical representation of the Novell Directory Services database on NetWare 4.0 and higher networks.
- NetBIOS Extended User Interface (NetBEUI)** — A simple transport program developed to support NetBIOS installations. NetBEUI is not routable, so it is not appropriate for larger networks.
- NetBIOS over TCP/IP (NBT)** — A network protocol in the TCP/IP stack that provides NetBIOS naming services.
- NetWare Core Protocol (NCP)** — The protocol used by CSNW to make file and print services requests of NetWare servers.
- Network Basic Input/Output System (NetBIOS)** — A client/server interprocess communication service developed by IBM in 1985. NetBIOS presents a relatively primitive mechanism for communication in client/server applications, but allows an easy implementation across various Microsoft Windows computers.
- Network Device Interface Specification (NDIS)** — Microsoft specification that defines parameters for loading more than one protocol on a network adapter.
- Network Dynamic Data Exchange (NetDDE)** — An interprocess communication mechanism developed by Microsoft to support the distribution of DDE applications over a network.
- network number** — The specific network identifier used by IPX for internal and network communication.
- Novell Directory Services (NDS)** — The hierarchical database used by NetWare 4.0 and higher servers to store network resource object configuration information.
- NWLink** — Microsoft's implementation of Novell's IPX/SPX protocol suite.
- Open Datalink Interface (ODI)** — Novell's specification for network device communication.
- Packet Internet Groper (PING)** — An IP-based utility that can be used to check network connectivity or to verify whether a specific host elsewhere on the network can be reached.
- Reverse Address Resolution Protocol (RARP)** — The IP protocol used to map from a physical MAC-layer address to a logical IP address.
- remote execution (rexec)** — The IP-based utility that permits a user on one machine to execute a program on another machine elsewhere on the network.
- remote shell (rsh)** — The IP-based utility that permits a user on one machine to enter a shell command on another machine on the network.
- Sequenced Packet Exchange (SPX)** — A connection-oriented protocol used in the NetWare environment when guaranteed delivery is required.
- Simple Mail Transport Protocol (SMTP)** — The IP-based messaging protocol and service that supports most Internet e-mail.

Simple Network Management Protocol (SNMP) — The IP-based network management protocol and service that makes it possible for management applications to poll network devices and permits devices to report on error or alert conditions to such applications.

subnet — A portion of a network that might or might not be a physically separate network. A subnet shares a network address with other parts of the network but is distinguished by a subnet number.

subnet mask — The number used to define which part of a computer's IP address denotes the host and which part denotes the network.

Telnet — The TCP/IP-based terminal emulation protocol used on IP-based networks to permit clients on one machine to attach to and operate on another machine on the network as if the other machines were terminals locally attached to a remote host.

Transmission Control Protocol/Internet Protocol (TCP/IP) — A suite of Internet protocols upon which the global Internet is based. TCP/IP is the default protocol for Windows XP.

Transmission Control Protocol (TCP) — The reliable, connection-oriented IP-based transport protocol that supports many of the most important IP services, including HTTP, SMTP, and FTP.

Trivial File Transport Protocol (TFTP) — A lightweight alternative to FTP, TFTP uses UDP to provide only simple get-and-put capabilities for file transfer on IP-based networks.

Universal Naming Convention (UNC) — A multivendor, multiplatform convention for identifying shared resources on a network.

User Datagram Protocol (UDP) — A lightweight, connectionless transport protocol used as an alternative to TCP in IP-based environments to supply faster, lower overhead access, primarily (but not exclusively) to local resources.

Windows Internet Name Service (WINS) — Service that provides NetBIOS-name-to-IP-address resolution.

REVIEW QUESTIONS

1. The _____ enables a system to determine which part of an IP address represents the host, and which part represents the network.
2. _____ is a TCP/IP service used to resolve host or domain names to addresses.
3. The _____ service can be used to automatically assign IP configurations to a computer.
4. The _____ file provides NetBIOS name-to-IP address resolution.
5. _____ is a TCP/IP protocol that is used for file manipulation.
6. By changing the _____, you alter the order in which services are accessed.

7. _____ is the Microsoft service that provides NetBIOS name to address resolution.
8. The current version of TCP/IP (IPv4) uses a/an _____ bit addressing scheme.
9. NDIS allows any number of adapters to be bound to any number of transport protocols. True or False?
10. Which of the following new networking features of Windows XP cannot be used on systems that are domain clients?
 - a. Network Bridging
 - b. Remote Assistance
 - c. Remote Desktop
 - d. Wireless networking
11. What are the restrictions for making a network connection part of a network bridge on Windows XP?
 - a. Not a dial-up connection
 - b. Not controlled by ICF
 - c. Not a wireless connection
 - d. Not controlled by ICS
12. Which Windows XP networking component allows a system to access shared resources?
 - a. TCP/IP
 - b. Workstation service
 - c. RPC
 - d. NetDDE
13. If you are assigned the IP address 172.16.1.1, what full class subnet mask is most likely the correct one to use?
 - a. 255.0.0.0
 - b. 255.255.0.0
 - c. 255.255.255.0
14. Which class of IP addresses offers the most flexibility with regard to subnetting by providing for the most number of hosts?
 - a. Class A
 - b. Class B
 - c. Class C

15. What should be placed on remote systems that connect to routed networks over slow WAN links?
 - a. NWLink
 - b. LMHOSTS
 - c. DNS
 - d. HOSTS
 - e. WinInet
16. Which TCP/IP command was designed to test the presence of a remote system?
 - a. Telnet
 - b. PING
 - c. ARP
 - d. Route
17. Which of the following is the static text-based equivalent of the Windows XP NetBIOS name to IP address resolution service?
 - a. HOSTS
 - b. LMHOSTS
 - c. DNS
 - d. WINS
18. If your network hosts the appropriate automatic addressing service, you do not need to manually configure TCP/IP to participate in a network. True or False?
19. Which of the following protocols is used to inquire if an address is reachable on the Internet?
 - a. SMTP
 - b. UTP
 - c. PING
 - d. IMAP
20. What IPC interfaces are used by Windows XP for file system access? (Choose all that apply.)
 - a. WinSock
 - b. named pipes
 - c. mailslots
 - d. OLE

21. Networking bridging offers what benefits?
 - a. Filtering
 - b. Communication between subnets without expensive hardware
 - c. Communication between networks of differing media and protocol
 - d. Full routing control
22. Remote Desktop can be used to invite another user to interact with your desktop environment in order to demonstrate how to perform some activity. True or False?
23. NDIS and ODI are technologies that provide for _____.
 - a. dynamic client configuration
 - b. distribution of driver software
 - c. binding of multiple protocols to multiple adapters
 - d. resolution of names to IP addresses
24. Which of the following will reduce broadcasts the most in a TCP/IP environment?
 - a. DNS
 - b. WINS
 - c. NWLink
 - d. DLC
25. TCP/IP is the most widely used protocol in the world. True or False?
26. All versions of NetWare utilize NDS. True or False?
27. Which of the following elements is part of Microsoft's NetWare environment for Windows XP Professional? (Choose all that apply.)
 - a. NWLink
 - b. CSNW
 - c. GSNW
 - d. NetWare File and Print Services
28. For IPX/SPX communication to succeed on a network, all computers must use the same frame type. True or False?
29. Which of the following NetWare protocols provides guaranteed packet delivery?
 - a. NWLink
 - b. IPX
 - c. SPX
 - d. NCP

30. When choosing a NetWare client for Windows XP, which of the following conditions should guide that choice? (Choose all that apply.)
- Always use the Microsoft Client for NetWare networks.
 - Always use the Novell 32-bit Windows client.
 - If there are more NetWare servers than Windows servers, or if native support for NDS and NetWare-aware applications is required, use the Novell 32-bit Windows client.
 - If there are more Windows servers than NetWare servers, or if native support for Active Directory and Windows applications is required, use the Microsoft Client for NetWare Networks.

HANDS-ON PROJECTS



Project 7-1

To view the status and properties of a Local Area Connection:



This hands-on project assumes your Windows XP Professional system is connected to a network.

- Open the **Network Connections** dialog box (**Start | Control Panel | Network Connections**). If the Control Panel is in Category View, select the Network and Internet Connections category, then click the Network Connections object.
- Select the **Local Area Connection** object.
- Select **File | Status**. This reveals the Local Area Connection Status dialog box. Notice the details provided on this dialog box: Connection Status, Duration, Speed, and Packets.
- Click the **Properties** button. This reveals the Local Area Connection Properties dialog box for this connection. Notice how this dialog box reveals the NIC involved with this connection and all of the services and protocols associated with this connection.
- Click **Cancel** to close the Local Area Connection Properties dialog box.
- Click **Close** to close the Local Area Connection Status dialog box.



Project 7-2

To use PING to test TCP/IP communications:



This hands-on project assumes you are connected to a TCP/IP network. You must know the IP address or host name or FQDN of at least one system on your network (or the Internet if you also have Internet access).

1. Open the **Command Prompt** (**Start** | **All Programs** | **Accessories** | **Command Prompt**).
2. Type **PING** *<IP address or name>* where *<IP address or name>* is the IP address of a system on your network, the name of a system on your network, or the domain name of a system on the Internet. Press **Enter**. You should see a statement similar to “Pinging 172.16.1.7 with 32 bytes of data:” followed by four lines listing whether a reply was received or a timeout occurred.
3. Type **exit** then press **Enter**.

7

Project 7-3

To view the HOSTS and LMHOSTS sample files:

1. Open Notepad (**Start** | **All Programs** | **Accessories** | **Notepad**).
2. Select **File** | **Open**.
3. Use the Open dialog box to locate and select the **\WINDOWS\system32\drivers\etc** directory.
4. Change the **Files of type** to **All Files** by using the pull-down list.
5. You should see a list of files in this folder. Select **hosts**, then click **Open**.
6. Scroll down through this file reading the information it provides. Do not make any changes to the file at this time.
7. Select **File** | **Open**. You should still be viewing the **\etc** directory.
8. Change the **Files of type** to **All Files** by using the pull-down list.
9. You should see a list of files in this folder. Select **lmhosts** or **lmhosts.sam**, then click **Open**.
10. Scroll down through this file reading the information it provides. Do not make any changes to the file at this time.
11. Select **File** | **Exit**.



Project 7-4

To configure TCP/IP:



The IP address of 172.16.1.1 and subnet mask of 255.255.255.0 can be replaced by your own assigned values.

1. Open Network Connections (**Start** | **Control Panel** | **Network Connections**).
2. Select the **Local Area Connection** object.
3. Select **File** | **Properties**. This reveals the Properties dialog box for the selected Local Area Connection object.
4. Select the **Internet Protocol (TCP/IP)** in the list of components.
5. Click **Properties**. This reveals the Internet Protocol (TCP/IP) Properties dialog box.
6. Select the **Use the following IP address** radio button.
7. Type in the IP address of **172.16.1.1**.
8. Type in the subnet mask of **255.255.255.0**.
9. Click **OK**.
10. Click **OK**.
11. Click the **File** menu, then click **Close**.
12. Reboot the system for the changes to take effect.



Project 7-5

To view network bindings:

1. Open Network Connections (**Start** | **Control Panel** | **Network Connections**). If the Control Panel is in Category View, select the Network and Internet Connections category, then click the Network Connections object.
2. Click the **Advanced** menu, then click **Advanced Settings**. This reveals the Advanced Settings dialog box where bindings are managed.
3. Select a connection from the connection box.
4. Notice the contents of the lower field where installed services and protocols are listed in their binding order.
5. Notice the items closer to the top of the list are bound in priority to those listed lower on the list.
6. Notice the checkbox beside each item that allows you to disable that service or protocol.
7. Click **Cancel** to ensure you've made no changes.
8. Click the **File** menu, then click **Close**.



Project 7-6

To send an invitation for Remote Assistance:



This hands-on project requires that the system have the Outlook Express or other e-mail system configured. This project also requires that you know the e-mail address of the teacher to invite.

1. Click **Start | Help and Support**. The Help and Support Center is displayed.
2. Click **Invite a friend to connect to your computer with Remote Assistance**. The Remote Assistance help page is displayed.
3. Click on **Invite someone to help you**. The Pick how you want to contact your assistant page is displayed.
4. In the Type an e-mail address text box, type in the e-mail address of the teacher to invite.
5. Click **Invite this person**. The E-mail an invitation page is displayed.
6. In the **From** field, type in the name to appear on the invitation if Administrator is not sufficient.
7. In the **Message** field, type in a message to the invitee, such as “Please help me.”
8. Click **Continue**.
9. Define the expiration time limit for this invitation, such as 30 minutes.
10. Be sure the **Require the recipient to use a password** checkbox is marked.
11. Provide a password and confirm the password. Be sure to remember what this password is and to provide it to the teacher. It is not wise to include the password in the e-mail message.
12. Click **Send Invitation**.
13. A confirmation box may appear asking whether you wish to send the message, click **Send** or **Yes**.
14. The Help and Support Center returns you to the Remote Assistance page, click **View invitation status**. A listing of the invitation you’ve sent appears.
15. Click the radio button beside your invitation, then click **Details**.
16. A dialog box with complete details about the invitation is displayed, click **Close**.



Do not use any of these options now, but for informational purposes, you should know that the Expire button instantly expires the invitation, the Resend button initiates resending the invitation, and the Delete button removes the invitation.

17. Click the **X** button in the title bar to close the Help and Support Center.



You may have to send the message manually from within Outlook.



Project 7-7

To respond to an invitation for Remote Assistance:



This hands-on project requires the following: that you work from another Windows XP system, that you have received the invitation from Hands-on Project 7-6, network connectivity between the teacher/assistant computer and the student/end-user computer, and that both computer system have Internet access.

1. On the teacher's computer, open an e-mail client, such as Outlook Express.
2. Locate the e-mail from the student.
3. Launch the attachment to initiate Remote Assistance.



The messages and attachments from Remote Assistance are easy to impersonate, so be sure that the attachment you launch is a valid Remote Assistance utility and not a malicious hacker tool.

4. The Remote Assistance tool launches, and prompts you for the password; type in the password provided by the student.
5. Click **Yes**.
6. On the student's computer, a pop-up dialog box appears asking if you want to allow the teacher to connect, click **Yes**.
7. The Remote Assistance control bar appears on the student's computer. The Remote Assistance desktop access window and control utility appears on the teacher's computer.
8. From either system, type in a short message in the **Message Entry** section, such as **What may I assist you with?**, then click **Send**.
9. On the teacher's computer, click **Take Control** from the top toolbar.
10. On the student's computer, click **Yes** when prompted whether to grant control of the computer.
11. On the teacher's computer, click **OK** when informed you have taken control.
12. On the teacher's computer open and close **Windows Explorer**. Notice that the movements made on the teacher's computer actually take effect on the student's computer.
13. On the teacher's computer, click **Disconnect** from the top tool bar.
14. On both computers, click **OK** when informed that Remote Assistance has been disconnected.
15. On both computers, click the **X** button on the title bar of Remote Assistance to close the interface.



Project 7-8

To install NWLink:

1. If you have not already done so, log on to your Windows XP Professional computer as Administrator.
2. Click **Start**, then right-click **My Network Places** and then select **Properties**.
3. Right-click **Local Area Connection** and then select **Properties**.
4. In the Local Area Connection Properties dialog box, click **Install**.
5. Select **Protocol** from the list of available components and then click **Add**.
6. Select **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** from the list.
7. Click **OK** to complete the installation. Note that you do not need to reboot the computer for this addition to take effect.
8. Click **Close** on the Local Area Connection dialog box.
9. Right-click again on the **Local Area Connection** icon and select **Properties** to configure NWLink. Note that NWLink NetBIOS has been added to the installed components list.
10. Select **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** from the list and then click **Properties**.
11. Enter an internal network number for the computer. Use any combination of up to six numbers and letters A–F. For example, 1FAD or 1999A.
12. Click the down arrow for the **Frame type** dropdown list and select a frame type. If you are in a classroom environment, select the frame type specified by the instructor.
13. Note that you must specify the Network number for the selected frame. Enter a network number in the space provided. If you are in a classroom environment, enter the network number specified by the instructor.
14. Click **OK** twice to complete the configuration. Note that the changes take effect immediately. If you are in a classroom environment, ensure that communications are available to computers with the same frame type and network number.
15. Close the Network and Dial-up Connections window.



Project 7-9

To install and configure Client Service for NetWare:

1. If you have not already done so, logon to your Windows XP Professional computer as Administrator.
2. Click **Start**, then right-click **My Network Places** and then select **Properties**.
3. Right-click **Local Area Connection** and then select **Properties**.
4. In the Local Area Connection Properties dialog box, click **Install**.

5. Select **Client** from the list of available components and then click **Add**. Note that the only client available to be installed is Client Service for NetWare.
6. Select **Client Service for NetWare** and then click **OK**. Click **Yes** to restart your computer when prompted to do so.
7. Logon to the computer as Administrator.
8. When prompted in the Select NetWare Logon window, follow your classroom instructions. You'll either click the Default Tree and Context radio button, and enter the default tree and context for your computer on the network, or provide a name for the Preferred Server to which the computer will connect (this latter element is selected by default).
9. Wait a moment while the configuration changes are made, then, if prompted, click **Yes** to restart the computer.
10. After the computer has restarted, log on to your Windows XP Professional computer as Administrator.
11. Open the Control Panel by selecting **Start | Control Panel**. Note that the CSNW icon appears.
12. Double-click the **CSNW** icon to open the Client Service for NetWare dialog box. Adjust the Print Options and Login Script Options as desired and click **OK**.
13. Note that you receive an information box telling you that the changes will take effect the next time you log in. Click **OK** to continue.
14. Close the Control Panel.

CASE PROJECTS

1. Describe the functions and features of TCP/IP included with Windows XP.
2. As a network administrator at XYZ Corp., you always hear about it when performance problems arise on the network. In the past two weeks, you've been involved in switching the network over from using NWLink exclusively to a mixture of NWLink and TCP/IP. You've installed TCP/IP on all Windows 2000 Server and Windows XP Professional systems, and made sure that all the machines are properly configured. Because the network is growing, and an additional cable segment has been added, with more planned for the future, you plan to switch entirely from NWLink to TCP/IP over time. All of a sudden, your users complain that the network has slowed dramatically. What steps can you take that might improve speed performance? Which machines should you make changes on and why?